

**THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
SOUTHERN DIVISION**

Atiya Abdulmalik, Francine Adams, Annemarie Amarena, Melissa Ames, Jamie Bannon, Robert Barbour, Joanne Barrett, Ann Bascom, Dana Bass, Paulette Beale, Kimberly Bentley, Catherine Berrahou, Michael Betit, Juliet Black, Darrell Black, Winnie Blackwell, Steven Bloom, Heidi Bodian, Bridget Bodie-Papino, Michelle Bonifacio, Candace Boston, Cory Bovair, Celia Bowman, Katesha Box, Miriam Boyd, Julia Boykin, Anitra Bradley, Brian Braid, Byron Brewer, Barbara Brooks, Dorothy Brooks, Adrienne Brown, David Bruemmer, Cheryl Butler-Adams, Kathrina Cajigal, Cole Callahan, Valerie Campanella, Alisha Campbell, Cayla Campbell, Claudia Canedo, Chastity Canfall, Elizabeth Capper, Arhonda Carlisle, Yvette Caruthers, Luke Castle, Chris Cervantes, Amy Chen, Kevin Cheng, Raphael Chieke, Cindy Chism, Nycole Chisum, Ryan Ciavarra, Rob Colletti, Brady Collins, Kevin Collins, Rita Connuck, Scott Coogan, Carol Cook, James Cook, Meghan Cook, Kristie Cooley, Laura Coombs, Cassandra Cooper, William Copeland, Jeri Covington, Kelly Cox, Ivette Crawford, Ebony Currie, Betty Dampier, Davidez Dampier, Barbara Dane, Julie Davis, Kimberly R Davis, Shanti Davis, Austin Delaney, Jenn Demarco, Sherry Denny, Benjamin Desantis, Mark Diefenbach, Tammy Doles, Nathlie Dowdell, Perkins Drake, Lula Draper, Eric Dubitsky, Tommy Dudley, Alexander Duff, India Dugat, Stephanie Dyer, Allison Eells, Romel Fajardo, Jeremaih Fanyui, Annette Fears, Arnold Fishon, Eric Fishon, Sara Flesch, Sharay Floyd, Donna Fontaine, Jeral Forger, Adam Fornal, Shaelyn Forrest, Arlona Fredrickson, Philip Friedman, Lisa Gadsby, Cindy Gaines, Christopher Galasso, Pablo Gallegos, Julie Ganuelas, Fae Garden, Mark Gardner, Mitchell Gerson, Kim Gibbs, John Gilmour, Robert Glass, Paula Glass, Maxine Glass, Kimberly Gomez, Billy Goodman, Lonja Green, Dale Grimes, Samir Gupta, Laurie Hansen, John Hariaczyi, Basimah Hasan, Philip Haskett, Andrew Hickner, Thomas Hickner,

Case No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Robin Hollingsworth, Paul Holloway, Mary Hopson, Talitha Huddleston, Gennell Hunter, Dustin Iagulli, Chasity Jackson, Christina Jackson, Tameka Jackson, Michael Jennings, Lisa Johnson, Shana Jordan, Teisha Jordan, Robert Keil, Raymond Kerkvliet, Marybeth Kern, Pegi Klaess, Robert Korn, Stanley Kubinski, Julius Kuperberg, Tina Lapene, Robin Lawler, Krystal Lear, Donna Level, Deborah Lewandowski, Courtney Lewis, Jahmelia Lewis, Tishaunda Lewis, Valerie Lewis, Violet Limen, Agnieszka Lizewska, Jay Lockaby, Melanie Lopez, Shayla Lowry, Juan Lozano, Elizabeth Lyons, Tiffany Maberry, Rita Mair, Charity Maldonado, Suzanne Mallon, Deann Mankell, Bryan Mantei, Pauline Marco, Leslie Martin, Mark Mason, Maria Masucci, Eric Mcpherson, Deborah Meade, Chloe Merjil, Collin Messer, Laura Messier, Cariss Milano, Shane Miller, Vickie Mondane, Gabrielle Moore, Jason Moore, Tanika Moore, John Moy, Albert Muick, Jose Munoz, Gwendolyn Murai, Maggie Murphy, Ron Musto, Amelia Naccarto-Coleman, Maria Naclerio, Sarah Newcomb, Dianna Nolan, Gerard Ohara, Sherita Olive-Miller, Sandra Ortner, Anita Overton-Smith, Alicia Page, Nikki Page, Rebecca Pageau, Kevin Parker, Michael Anthony Partland, Douglas Patton, Shanisha Perkins, Patrice Perrier, Yaroslava Petraitis, Terri Pettiford, Michelle Pfannenstiel, Sean Phillips, Patrick Plank, Emily Poltrack, George Pouliot, Walter Powell, Andrea Preston, Tammie Pry, David Rado, Frank Ragan, Giorgio Ramirez, Lupe Ramos, Nicole Regne, Donna Riggins, Steve Risinger, Marvin Roberson, Dominique Robertson, Lamarkis Robinson, Nick Robinson, Lanny Rodgers, Robert Rodriguez, Kathleen Romeo, Elizabeth Rosch, Stacey Rowland, Paul Rozzo, Steven Ruga, Joshua Ruhlman, Niesha Rush, Brittany Rushing, Stacy Ryan, Adam Sanderson, Luis Santos, Stephen Sawyer, Holly Schmidt, Terry Senn, Hiren Shah, Svetlana Shtofmakher, Jose Siandre, Lenord Simmons, Janet Simonitsch, Illya Singh, Lori Smallwood, Julissa Solano, Steven Spagnolo, Michael Spain, Donald Springer, Shelli Stapp, Bahasha Stigall, Tammy Stiller, Daniel Stinson, Debra Stolte, Simon Sum, Jennifer Sykes, Yanina Szenkman, Gerald Taylor,

Melissa Taylor, Nicole Theiss, Carla Theriot, Roy Thompson, Valerie Tolliver, Matthew Tragarz, Michael Traugott, Ryan Truskowski, Martin Turnauer, Stella Ureno, Audrey Varner, Leo Varshavsky, David Viggiano, Anne Vitasek, April Vrtis, Bryan Wallace, James Walton, Andrew Walts, Clara White, Matthew White, Randolph White, Octavia Wilkerson, Dolly Wright, Chris Wright, Fugong Wu, Debra Yokoyama, Glenn Young, Brittany Young, Jacqueline Zenon, Individually and on Behalf of All Others Similarly Situated,

Plaintiffs,

v.

MARRIOTT INTERNATIONAL, INC. and
STARWOOD HOTELS & RESORTS
WORLDWIDE, LLC.,

Defendants.

CLASS ACTION COMPLAINT

1. Plaintiffs¹ individually and on behalf of a class of all persons similarly situated (the “Class” or “Class Members”), bring this class action against Defendants Marriott International, Inc. and Starwood Hotels & Resorts Worldwide, LLC (collectively, “Marriott” or “Defendants”) seeking equitable relief and damages as set forth below.

PRELIMINARY STATEMENT

2. Plaintiffs bring this action against Marriott for its failure in securing and safeguarding their personal and financial information, which Marriott required its customers to provide when they made reservations, checked into hotels, used one of its loyalty programs, or made purchases at dining or retail operations within its hotels. Plaintiffs further allege that Marriott failed to adequately notify Plaintiffs and Class Members in a timely manner that their PII

¹ Plaintiffs refer to the individuals referenced in the caption above and described more fully in paragraphs 10 to 304 below.

had been stolen in violation of common law duties and numerous consumer protection statutes.

3. On November 30, 2018, Marriott announced that it had discovered a data breach of its reservation and database systems where unauthorized parties since 2014 accessed the guest reservation system and acquired the private information of up to 500 million guests (the “Breach”). For approximately 327 million of these guests, the personally identifiable information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest account information, date of birth, gender, arrival and departure information, reservation date, communication preferences, payment card numbers, and payment card expiration dates (collectively, “PII”).

4. The Breach was reasonably foreseeable given that numerous other hotel chains in the hospitality industry, including Starwood, maintained inadequate data security resulting in prior data breaches and other data security incidents.

5. Marriott failed to take adequate and reasonable measures to secure its customers’ PII collected in transactions and stored on its databases.

6. This Class Action Complaint is filed on behalf of all persons in the United States, described more fully in the following sections, whose PII was compromised in the Breach.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over the state law claims asserted here pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), since some of the Class Members are citizens of a State different from Marriott, there are more than 100 putative class members, and the amount in controversy exceeds \$5 million.

8. This Court has personal jurisdiction over the Parties because Marriott is headquartered in Maryland and conduct a major part of their national operations with regular and continuous business activity in Maryland.

9. Venue is proper under 28 U.S.C. § 1391(c) because Marriott is a corporation that

does business in and is subject to personal jurisdiction in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claims in this action occurred in or emanated from this District, including the decisions made by Marriott's governance and management personnel that led to the breach.

PARTIES

10. Plaintiff Atiya Abdulmalik is a resident and citizen of Virginia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

11. Plaintiff Francine Adams is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

12. Plaintiff Annemarie Amarena is a resident and citizen of Connecticut who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach. Ms. Amarena provided her passport information to Marriott in connection with a stay at a Starwood property outside of the United States.

13. Plaintiff Melissa Ames is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

14. Plaintiff Jamie Bannon is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

15. Plaintiff Robert Barbour is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

16. Plaintiff Joanne Barrett is a resident and citizen of Massachusetts who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

17. Plaintiff Ann Bascom is a resident and citizen of Maryland who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

18. Plaintiff Dana Bass is a resident and citizen of Indiana who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

19. Plaintiff Paulette Beale is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

20. Plaintiff Kimberly Bentley is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

21. Plaintiff Catherine Berrahou is a resident and citizen of Michigan who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

22. Plaintiff Michael Betit is a resident and citizen of New York who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

23. Plaintiff Juliet Black is a resident and citizen of North Carolina who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

24. Plaintiff Darrell Black is a resident and citizen of Virginia who has stayed at a

Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

25. Plaintiff Winnie Blackwell is a resident and citizen of North Carolina who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

26. Plaintiff Steven Bloom is a resident and citizen of Illinois who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

27. Plaintiff Heidi Bodian is a resident and citizen of Connecticut who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach. Ms. Bodian provided her passport information to Marriott in connection with a stay at a Starwood property outside of the United States.

28. Plaintiff Bridget Bodie-Papino is a resident and citizen of New Jersey who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

29. Plaintiff Michelle Bonifacio is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

30. Plaintiff Candace Boston is a resident and citizen of Maryland who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

31. Plaintiff Cory Bovair is a resident and citizen of North Carolina who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

32. Plaintiff Celia Bowman is a resident and citizen of Colorado who has stayed at a

Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

33. Plaintiff Katesha Box is a resident and citizen of Georgia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

34. Plaintiff Miriam Boyd is a resident and citizen of Alabama who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

35. Plaintiff Julia Boykin is a resident and citizen of South Carolina who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

36. Plaintiff Anitra Bradley is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

37. Plaintiff Brian Braid is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

38. Plaintiff Byron Brewer is a resident and citizen of Alabama who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

39. Plaintiff Barbara Brooks is a resident and citizen of Indiana who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

40. Plaintiff Dorothy Brooks is a resident and citizen of Michigan who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information

compromised as a result of the Breach.

41. Plaintiff Adrienne Brown is a resident and citizen of Tennessee who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

42. Plaintiff David Bruemmer is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

43. Plaintiff Cheryl Butler-Adams is a resident and citizen of Nevada who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

44. Plaintiff Kathrina Cajigal is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

45. Plaintiff Cole Callahan is a resident and citizen of Rhode Island who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

46. Plaintiff Valerie Campanella is a resident and citizen of New Jersey who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

47. Plaintiff Alisha Campbell is a resident and citizen of Georgia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

48. Plaintiff Cayla Campbell is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

49. Plaintiff Claudia Canedo is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

50. Plaintiff Chastity Canfall is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

51. Plaintiff Elizabeth Capper is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach. Ms. Capper provided her passport information to Marriott in connection with a stay at a Starwood property outside of the United States.

52. Plaintiff Arhonda Carlisle is a resident and citizen of Minnesota who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

53. Plaintiff Yvette Caruthers is a resident and citizen of Georgia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

54. Plaintiff Luke Castle is a resident and citizen of Louisiana who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

55. Plaintiff Chris Cervantes is a resident and citizen of Colorado who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

56. Plaintiff Amy Chen is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

57. Plaintiff Kevin Cheng is a resident and citizen of New York who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

58. Plaintiff Raphael Chieke is a resident and citizen of Pennsylvania who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

59. Plaintiff Cindy Chism is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

60. Plaintiff Nycole Chisum is a resident and citizen of Georgia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

61. Plaintiff Ryan Ciavarra is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

62. Plaintiff Rob Colletti is a resident and citizen of Arizona who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

63. Plaintiff Brady Collins is a resident and citizen of Illinois who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

64. Plaintiff Kevin Collins is a resident and citizen of Illinois who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

65. Plaintiff Rita Connuck is a resident and citizen of Georgia who has stayed at a

Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

66. Plaintiff Scott Coogan is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

67. Plaintiff Carol Cook is a resident and citizen of Maryland who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

68. Plaintiff James Cook is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach. Mr. Cook provided his passport information to Marriott in connection with a stay at a Starwood property outside of the United States.

69. Plaintiff Meghan Cook is a resident and citizen of North Carolina who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

70. Plaintiff Kristie Cooley is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

71. Plaintiff Laura Coombs is a resident and citizen of Maryland who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

72. Plaintiff Cassandra Cooper is a resident and citizen of Georgia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

73. Plaintiff William Copeland is a resident and citizen of Kentucky who has stayed at

a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

74. Plaintiff Jeri Covington is a resident and citizen of Missouri who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

75. Plaintiff Kelly Cox is a resident and citizen of Oregon who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

76. Plaintiff Ivette Crawford is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

77. Plaintiff Ebony Currie is a resident and citizen of Maryland who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

78. Plaintiff Betty Dampier is a resident and citizen of Mississippi who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

79. Plaintiff Davidez Dampier is a resident and citizen of Pennsylvania who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

80. Plaintiff Barbara Dane is a resident and citizen of Massachusetts who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

81. Plaintiff Julie Davis is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised

as a result of the Breach.

82. Plaintiff Kimberly R Davis is a resident and citizen of Illinois who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

83. Plaintiff Shanti Davis is a resident and citizen of Michigan who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

84. Plaintiff Austin Delaney is a resident and citizen of New York who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

85. Plaintiff Jenn Demarco is a resident and citizen of Pennsylvania who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

86. Plaintiff Sherry Denny is a resident and citizen of Arizona who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

87. Plaintiff Benjamin Desantis is a resident and citizen of North Carolina who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

88. Plaintiff Mark Diefenbach is a resident and citizen of New York who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

89. Plaintiff Tammy Doles is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

90. Plaintiff Nathlie Dowdell is a resident and citizen of Georgia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

91. Plaintiff Perkins Drake is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

92. Plaintiff Lula Draper is a resident and citizen of Mississippi who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

93. Plaintiff Eric Dubitsky is a resident and citizen of Ohio who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

94. Plaintiff Tommy Dudley is a resident and citizen of North Carolina who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

95. Plaintiff Alexander Duff is a resident and citizen of Washington who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

96. Plaintiff India Dugat is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

97. Plaintiff Stephanie Dyer is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

98. Plaintiff Allison Eells is a resident and citizen of North Carolina who has stayed at

a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

99. Plaintiff Romel Fajardo is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

100. Plaintiff Jeremaih Fanyui is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

101. Plaintiff Julius Farrar is a resident and citizen of Utah who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

102. Plaintiff Annette Fears is a resident and citizen of Georgia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

103. Plaintiff Arnold Fishon is a resident and citizen of New York who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

104. Plaintiff Eric Fishon is a resident and citizen of New York who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

105. Plaintiff Sara Flesch is a resident and citizen of Illinois who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

106. Plaintiff Sharay Floyd is a resident and citizen of Alabama who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information

compromised as a result of the Breach.

107. Plaintiff Donna Fontaine is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

108. Plaintiff Jeral Forger is a resident and citizen of New York who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

109. Plaintiff Adam Fornal is a resident and citizen of Wisconsin who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

110. Plaintiff Shaelyn Forrest is a resident and citizen of Virginia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

111. Plaintiff Arlona Fredrickson is a resident and citizen of Iowa who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

112. Plaintiff Philip Friedman is a resident and citizen of Maryland who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

113. Plaintiff Lisa Gadsby is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

114. Plaintiff Cindy Gaines is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

115. Plaintiff Christopher Galasso is a resident and citizen of New York who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

116. Plaintiff Pablo Gallegos is a resident and citizen of Colorado who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

117. Plaintiff Julie Ganuelas is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

118. Plaintiff Fae Garden is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

119. Plaintiff Mark Gardner is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

120. Plaintiff Mitchell Gerson is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

121. Plaintiff Kim Gibbs is a resident and citizen of South Carolina who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

122. Plaintiff John Gilmour is a resident and citizen of Illinois who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

123. Plaintiff Robert Glass is a resident and citizen of California who has stayed at a

Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

124. Plaintiff Paula Glass is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

125. Plaintiff Maxine Glass is a resident and citizen of Tennessee who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

126. Plaintiff Kimberly Gomez is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

127. Plaintiff Billy Goodman is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

128. Plaintiff Lonja Green is a resident and citizen of Delaware who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

129. Plaintiff Dale Grimes is a resident and citizen of Arizona who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

130. Plaintiff Samir Gupta is a resident and citizen of New York who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

131. Plaintiff Laurie Hansen is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information

compromised as a result of the Breach.

132. Plaintiff John Hariaczyi is a resident and citizen of New York who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

133. Plaintiff Basimah Hasan is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

134. Plaintiff Philip Haskett is a resident and citizen of Missouri who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

135. Plaintiff Andrew Hickner is a resident and citizen of New Jersey who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

136. Plaintiff Thomas Hickner is a resident and citizen of Michigan who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

137. Plaintiff Robin Hollingsworth is a resident and citizen of Michigan who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

138. Plaintiff Paul Holloway is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

139. Plaintiff Mary Hopson is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

140. Plaintiff Talitha Huddleston is a resident and citizen of Georgia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

141. Plaintiff Gennell Hunter is a resident and citizen of Washington who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

142. Plaintiff Dustin Iagulli is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

143. Plaintiff Chasity Jackson is a resident and citizen of Kansas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

144. Plaintiff Christina Jackson is a resident and citizen of Maryland who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

145. Plaintiff Tameka Jackson is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

146. Plaintiff Michael Jennings is a resident and citizen of Tennessee who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

147. Plaintiff Lisa Johnson is a resident and citizen of Ohio who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

148. Plaintiff Shana Jordan is a resident and citizen of North Carolina who has stayed at

a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

149. Plaintiff Teisha Jordan is a resident and citizen of Pennsylvania who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

150. Plaintiff Robert Keil is a resident and citizen of Minnesota who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

151. Plaintiff Raymond Kerkvliet is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

152. Plaintiff Marybeth Kern is a resident and citizen of Pennsylvania who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

153. Plaintiff Pegi Klaess is a resident and citizen of Alabama who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

154. Plaintiff Robert Korn is a resident and citizen of Kansas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

155. Plaintiff Stanley Kubinski is a resident and citizen of Massachusetts who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

156. Plaintiff Julius Kuperberg is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information

compromised as a result of the Breach.

157. Plaintiff Tina Lapene is a resident and citizen of Louisiana who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

158. Plaintiff Robin Lawler is a resident and citizen of Virginia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

159. Plaintiff Krystal Lear is a resident and citizen of Ohio who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

160. Plaintiff Donna Level is a resident and citizen of Georgia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

161. Plaintiff Deborah Lewandowski is a resident and citizen of Michigan who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

162. Plaintiff Courtney Lewis is a resident and citizen of Virginia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

163. Plaintiff Jahmelia Lewis is a resident and citizen of Georgia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

164. Plaintiff Tishaunda Lewis is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

165. Plaintiff Valerie Lewis is a resident and citizen of Virginia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

166. Plaintiff Violet Limen is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

167. Plaintiff Agnieszka Lizewska is a resident and citizen of New Jersey who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

168. Plaintiff Jay Lockaby is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

169. Plaintiff Melanie Lopez is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

170. Plaintiff Shayla Lowry is a resident and citizen of Georgia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

171. Plaintiff Juan Lozano is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

172. Plaintiff Elizabeth Lyons is a resident and citizen of Arkansas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

173. Plaintiff Tiffany Maberry is a resident and citizen of Georgia who has stayed at a

Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

174. Plaintiff Rita Mair is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

175. Plaintiff Charity Maldonado is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

176. Plaintiff Suzanne Mallon is a resident and citizen of Illinois who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

177. Plaintiff Deann Mankell is a resident and citizen of Missouri who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

178. Plaintiff Bryan Mantei is a resident and citizen of Wisconsin who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

179. Plaintiff Pauline Marco is a resident and citizen of West Virginia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

180. Plaintiff Leslie Martin is a resident and citizen of Washington who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

181. Plaintiff Mark Mason is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information

compromised as a result of the Breach.

182. Plaintiff Maria Masucci is a resident and citizen of Massachusetts who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

183. Plaintiff Eric Mcpherson is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach. Mr. McPherson provided his passport information to Marriott in connection with a stay at a Starwood property outside of the United States.

184. Plaintiff Deborah Meade is a resident and citizen of New Jersey who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

185. Plaintiff Chloe Merjil is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

186. Plaintiff Collin Messer is a resident and citizen of Ohio who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

187. Plaintiff Laura Messier is a resident and citizen of Rhode Island who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

188. Plaintiff Cariss Milano is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

189. Plaintiff Shane Miller is a resident and citizen of Mississippi who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information

compromised as a result of the Breach.

190. Plaintiff Vickie Mondane is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

191. Plaintiff Gabrielle Moore is a resident and citizen of North Carolina who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

192. Plaintiff Jason Moore is a resident and citizen of District of Columbia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

193. Plaintiff Tanika Moore is a resident and citizen of Nebraska who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

194. Plaintiff John Moy is a resident and citizen of New York who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

195. Plaintiff Albert Muick is a resident and citizen of Pennsylvania who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

196. Plaintiff Jose Munoz is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

197. Plaintiff Gwendolyn Murai is a resident and citizen of Hawaii who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

198. Plaintiff Maggie Murphy is a resident and citizen of North Carolina who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

199. Plaintiff Ron Musto is a resident and citizen of Pennsylvania who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

200. Plaintiff Amelia Naccarto-Coleman is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

201. Plaintiff Maria Naclerio is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

202. Plaintiff Sarah Newcomb is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

203. Plaintiff Dianna Nolan is a resident and citizen of New York who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

204. Plaintiff Gerard Ohara is a resident and citizen of South Carolina who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

205. Plaintiff Sherita Olive-Miller is a resident and citizen of Iowa who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

206. Plaintiff Sandra Ortner is a resident and citizen of Missouri who has stayed at a

Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

207. Plaintiff Anita Overton-Smith is a resident and citizen of Georgia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

208. Plaintiff Alicia Page is a resident and citizen of New Jersey who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

209. Plaintiff Nikki Page is a resident and citizen of Arizona who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

210. Plaintiff Rebecca Pageau is a resident and citizen of North Carolina who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

211. Plaintiff Kevin Parker is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

212. Plaintiff Michael Anthony Partland is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

213. Plaintiff Douglas Patton is a resident and citizen of Michigan who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

214. Plaintiff Shanisha Perkins is a resident and citizen of Oklahoma who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information

compromised as a result of the Breach.

215. Plaintiff Patrice Perrier is a resident and citizen of Maryland who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

216. Plaintiff Yaroslava Petraitis is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

217. Plaintiff Terri Pettiford is a resident and citizen of Georgia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

218. Plaintiff Michelle Pfannenstiel is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

219. Plaintiff Sean Phillips is a resident and citizen of Arkansas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

220. Plaintiff Patrick Plank is a resident and citizen of Minnesota who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

221. Plaintiff Emily Poltrack is a resident and citizen of Massachusetts who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

222. Plaintiff George Pouliot is a resident and citizen of North Carolina who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

223. Plaintiff Walter Powell is a resident and citizen of Michigan who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

224. Plaintiff Andrea Preston is a resident and citizen of Massachusetts who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

225. Plaintiff Tammie Pry is a resident and citizen of Illinois who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

226. Plaintiff David Rado is a resident and citizen of Connecticut who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

227. Plaintiff Frank Ragan is a resident and citizen of Delaware who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

228. Plaintiff Giorgio Ramirez is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

229. Plaintiff Lupe Ramos is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

230. Plaintiff Nicole Regne is a resident and citizen of New York who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

231. Plaintiff Donna Riggins is a resident and citizen of South Carolina who has stayed

at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

232. Plaintiff Steve Risinger is a resident and citizen of Washington who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

233. Plaintiff Marvin Roberson is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

234. Plaintiff Dominique Robertson is a resident and citizen of Maryland who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

235. Plaintiff Lamarkis Robinson is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

236. Plaintiff Nick Robinson is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

237. Plaintiff Lanny Rodgers is a resident and citizen of Pennsylvania who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

238. Plaintiff Robert Rodriguez is a resident and citizen of Indiana who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

239. Plaintiff Kathleen Romeo is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information

compromised as a result of the Breach.

240. Plaintiff Elizabeth Rosch is a resident and citizen of Illinois who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

241. Plaintiff Stacey Rowland is a resident and citizen of North Carolina who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

242. Plaintiff Paul Rozzo is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

243. Plaintiff Steven Ruga is a resident and citizen of Virginia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

244. Plaintiff Joshua Ruhlman is a resident and citizen of Michigan who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

245. Plaintiff Niesha Rush is a resident and citizen of Mississippi who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

246. Plaintiff Brittany Rushing is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

247. Plaintiff Stacy Ryan is a resident and citizen of New York who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

248. Plaintiff Adam Sanderson is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

249. Plaintiff Luis Santos is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

250. Plaintiff Stephen Sawyer is a resident and citizen of South Carolina who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

251. Plaintiff Holly Schmidt is a resident and citizen of Ohio who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

252. Plaintiff Terry Senn is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

253. Plaintiff Hiren Shah is a resident and citizen of Michigan who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

254. Plaintiff Svetlana Shtofmakher is a resident and citizen of New Jersey who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

255. Plaintiff Jose Siandre is a resident and citizen of New Jersey who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

256. Plaintiff Lenord Simmons is a resident and citizen of Florida who has stayed at a

Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

257. Plaintiff Janet Simonitsch is a resident and citizen of Missouri who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

258. Plaintiff Illya Singh is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

259. Plaintiff Lori Smallwood is a resident and citizen of Ohio who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

260. Plaintiff Julissa Solano is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

261. Plaintiff Steven Spagnolo is a resident and citizen of Pennsylvania who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

262. Plaintiff Michael Spain is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

263. Plaintiff Donald Springer is a resident and citizen of Pennsylvania who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

264. Plaintiff Shelli Stapp is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information

compromised as a result of the Breach.

265. Plaintiff Bahasha Stigall is a resident and citizen of Mississippi who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

266. Plaintiff Tammy Stiller is a resident and citizen of Georgia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

267. Plaintiff Daniel Stinson is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

268. Plaintiff Debra Stolte is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

269. Plaintiff Simon Sum is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

270. Plaintiff Jennifer Sykes is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

271. Plaintiff Yanina Szenkman is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

272. Plaintiff Gerald Taylor is a resident and citizen of Michigan who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

273. Plaintiff Melissa Taylor is a resident and citizen of Louisiana who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

274. Plaintiff Nicole Theiss is a resident and citizen of Ohio who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

275. Plaintiff Carla Theriot is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

276. Plaintiff Roy Thompson is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

277. Plaintiff Valerie Tolliver is a resident and citizen of Alabama who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

278. Plaintiff Matthew Tragarz is a resident and citizen of Tennessee who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

279. Plaintiff Michael Traugott is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

280. Plaintiff Ryan Truskowski is a resident and citizen of Michigan who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

281. Plaintiff Martin Turnauer is a resident and citizen of South Carolina who has stayed

at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

282. Plaintiff Stella Ureno is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

283. Plaintiff Audrey Varner is a resident and citizen of Ohio who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

284. Plaintiff Leo Varshavsky is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

285. Plaintiff David Viggiano is a resident and citizen of Georgia who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

286. Plaintiff Anne Vitasek is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

287. Plaintiff April Vrtis is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

288. Plaintiff Bryan Wallace is a resident and citizen of Michigan who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

289. Plaintiff James Walton is a resident and citizen of California who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information

compromised as a result of the Breach.

290. Plaintiff Andrew Walts is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

291. Plaintiff Clara White is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

292. Plaintiff Matthew White is a resident and citizen of Rhode Island who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

293. Plaintiff Randolph White is a resident and citizen of Montana who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

294. Plaintiff Octavia Wilkerson is a resident and citizen of Illinois who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

295. Plaintiff Dolly Wright is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

296. Plaintiff Chris Wright is a resident and citizen of Tennessee who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

297. Plaintiff Fugong Wu is a resident and citizen of Texas who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

298. Plaintiff Debra Yokoyama is a resident and citizen of Colorado who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

299. Plaintiff Glenn Young is a resident and citizen of Arizona who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

300. Plaintiff Brittany Young is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

301. Plaintiff Jacqueline Zenon is a resident and citizen of Florida who has stayed at a Starwood property during the relevant time period and subsequently had Personal Information compromised as a result of the Breach.

302. Marriott International, Inc. is a Delaware corporation with its headquarters and principal place of business in this District at 10400 Fernwood Road, Bethesda, Maryland 20817.

303. Marriott Starwood Hotels & Resorts Worldwide, LLC is incorporated under the laws of the State of Maryland, with its principal place of business at 10400 Fernwood Road, Bethesda, Maryland 20817.

STATEMENT OF FACTS

304. The Marriott hotel chain operates more than 6,700 properties. Marriott operates and franchises hotels and licenses vacation ownership resorts all around the world. The company is headquartered outside of Washington, D.C. in Bethesda, Maryland.

305. In September 2016, Marriott completed a \$13 billion acquisition of Starwood Hotels & Resorts Worldwide, to create the world's largest hotel chain. Starwood brands include W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft

Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton and Design Hotels and Starwood branded timeshare properties.

306. Marriott Group Global Privacy Statement available on marriott.com provides:

This Privacy Statement describes the privacy practices of the Marriott Group for data that we collect:

- through websites operated by us from which you are accessing this Privacy Statement, including Marriott.com and other websites owned or controlled by the Marriott Group (collectively, the “**Websites**”)
- through the software applications made available by us for use on or through computers and mobile devices (the “**Apps**”)
- through our social media pages that we control from which you are accessing this Privacy Statement (collectively, our “**Social Media Pages**”)
- through HTML-formatted email messages that we send you that link to this Privacy Statement and through your communications with us
- when you visit or stay as a guest at one of our properties, or through other offline interactions

Collectively, we refer to the Websites, the Apps and our Social Media Pages, as the “**Online Services**” and, together with offline channels, the “**Services.**” By using the Services, you agree to the terms and conditions of this Privacy Statement.

307. With respect to “Collection of Personal Data,” the policy provides as follows:

“**Personal Data**” are data that identify you as an individual or relate to an identifiable individual.

At touchpoints throughout your guest journey, we collect Personal Data in accordance with law, such as:

- Name
- Gender
- Postal address
- Telephone number
- Email address
- Credit and debit card number or other payment data
- Financial information in limited circumstances
- Language preference
- Date and place of birth
- Nationality, passport, visa or other government-issued identification data
- Important dates, such as birthdays, anniversaries and special occasions

- Membership or loyalty program data (including co-branded payment cards, travel partner program affiliations)
- Employer details
- Travel itinerary, tour group or activity data
- Prior guest stays or interactions, goods and services purchased, special service and amenity requests
- Geolocation information
- Social media account ID, profile photo and other data publicly available, or data made available by linking your social media and loyalty accounts

In more limited circumstances, we also may collect:

- Data about family members and companions, such as names and ages of children
- Biometric data, such as digital images
- Images and video and audio data via: (a) security cameras located in public areas, such as hallways and lobbies, in our properties; and (b) body-worn cameras carried by our loss prevention officers and other security personnel
- Guest preferences and personalized data (“**Personal Preferences**”), such as your interests, activities, hobbies, food and beverage choices, services and amenities of which you advise us or which we learn about during your visit

If you submit any Personal Data about other people to us or our Service Providers (e.g., if you make a reservation for another individual), you represent that you have the authority to do so and you permit us to use the data in accordance with this Privacy Statement.

308. The privacy policy also represents that “We seek to use reasonable organizational, technical and administrative measures to protect Personal Data.”

309. On November 30, 2018, Marriott announced that for four years unauthorized parties maintained access to its reservation systems which held the PII of up to 500 million customers, including Plaintiffs and Class Members.

310. Marriott was alerted to an attempt to access the Starwood guest reservation database in the United States on September 8, 2018. During the investigation, Marriott learned that there had been unauthorized access to the Starwood network since 2014. Marriott also discovered that an unauthorized party had copied and encrypted information from the Starwood guest

reservation database. The press release stated:

The company has not finished identifying duplicate information in the database, but believes it contains information on up to approximately 500 million guests who made a reservation at a Starwood property. For approximately 327 million of these guests, the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest (“SPG”) account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes payment card numbers and payment card expiration dates, but the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-128). There are two components needed to decrypt the payment card numbers, and at this point, Marriott has not been able to rule out the possibility that both were taken. For the remaining guests, the information was limited to name and sometimes other data such as mailing address, email address, or other information.

311. Marriott also acknowledged the Breach in a Form 8-K filing with the Securities and Exchange Commission.

A. Marriott’s Security Protocols Were Insufficient

312. Marriott maintained insufficient and inadequate data security policies, procedures, and practices to protect the payment information of Plaintiffs and the Class. It is well known, and the subject of many media reports, that PII is highly coveted and a frequent target of hackers. Despite well-publicized litigation and frequent public announcements of data breaches, Marriott maintained insufficient and inadequate data security policies, procedures, and practices to protect the PII of Plaintiffs and the Class.

313. After the public became aware of this massive Breach, Marriott’s Chief Executive Officer, Arne Sorenson, admitted that “[Marriott] fell short of what our guests deserve and what we expect of ourselves.”²

314. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The one year of credit monitoring

² *Marriott Breach Exposes Data of Up to 500 Million Guests*, <https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html> (last accessed Dec. 18, 2018).

offered by Marriott is entirely insufficient and inadequate, in part, because identity thieves are aware that victims of a data breach are on heightened alert immediately following a data breach announcement, often times resulting in identity thieves waiting months or years to utilize the acquired information. The Class is incurring and will continue to incur damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

B. Plaintiffs and the Class Suffered Damages

315. The Breach was a direct and proximate result of Marriott's failure to properly safeguard, protect, and monitor Plaintiffs' and Class' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law. The Breach was also a result of Marriott's failure in establishing and implementing appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

316. Plaintiffs' and Class Members' PII is private and sensitive in nature and was inadequately protected by Marriott. Marriott did not obtain Plaintiffs' and Class Members' consent to disclose their PII as required by applicable law and industry standards.

317. As a direct and proximate result of Marriott's wrongful action and inaction and the resulting data breach, as well as Marriott's unreasonable failure to timely identify the intrusion, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the subject Breach on their lives by, among other things, spending time and/or money placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely

reviewing and monitoring their credit reports and accounts for unauthorized activity.

318. Marriott's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including, but not limited to, the following:

- a. Theft and other misuse of their PII;
- b. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;
- c. The imminent and impending injury flowing from the sale of Plaintiffs' and Class Members' PII on the Internet black market;
- d. The untimely and inadequate notification of the Breach;
- e. The improper disclosure of their PII;
- f. Loss of privacy;
- g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;
- h. Ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;
- i. Overpayments to Marriott for booking and purchase during the Breach period in that a portion of the price paid for such booking by Plaintiffs and Class Members to Marriott was for the costs of reasonable and adequate safeguards and security measures that would protect customers' PII, which Marriott did not implement and, as a result, Plaintiffs and Class Members did not receive what they paid for and were overcharged by Marriott; and
- j. Deprivation of rights they possess under the state and federal law.

CLASS ALLEGATIONS

319. Plaintiffs bring this complaint on behalf of themselves and the following Class

Members (“Nationwide Class”):

All persons whose Personally Identifiable Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

320. Plaintiffs Boyd, Brewer, Floyd, Klaess, and Tolliver (“Alabama Plaintiffs”) also seek certification of the following state subclass (“Alabama Subclass”):

All persons residing in Alabama whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

321. Plaintiffs Colletti, Denny, Grimes, Nikki Page, and Glenn Young (“Arizona Plaintiffs”) also seek certification of the following state subclass (“Arizona Subclass”):

All persons residing in Arizona whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

322. Plaintiffs Lyons and Phillips (“Arkansas Plaintiffs”) also seek certification of the following state subclass (“Arkansas Subclass”):

All persons residing in Arkansas whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

323. Plaintiffs Ames, Barbour, Beale, Bradley, Braid, Cajigal, Canedo, Chen, Cooley, Drake, Gadsby, Gaines, Ganuelas, Paula Glass, Robert Glass, Goodman, Hansen, Holloway, Hopson, Lopez, Lozano, Maldonado, Merjil, Milano, Mondane, Munoz, Naccarto-Coleman, Petraitis, Ramos, Roberson, Santos, Solano, Stapp, Sum, Ureno, Varshavsky, Vrtis, and Walton (“California Plaintiffs”) also seek certification of the following state subclass (“California Subclass”):

All persons residing in California whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

324. Plaintiffs Bowman, Cervantes, Gallegos, and Yokoyama (“Colorado Plaintiffs”) also seek certification of the following state subclass (the “Colorado Subclass”):

All persons residing in Colorado whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

325. Plaintiffs Amarena, Bodian, and Rado (“Connecticut Plaintiffs”) also seek certification of the following state subclass (the “Connecticut Subclass”):

All persons residing in Connecticut whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

326. Plaintiffs Green, and Ragan (“Delaware Plaintiffs”) also seek certification of the following subclass (“Delaware Subclass”):

All persons residing in the Delaware whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

327. Plaintiff Jason Moore (“District of Columbia Plaintiff”) also seeks certification of the following subclass (“District of Columbia Subclass”):

All persons residing in the District of Columbia whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

328. Plaintiffs Adams, Bannon, Bentley, Bonifacio, Bruemmer, Canfall, Coogan, Crawford, Doles, Dyer, Fajardo, Fontaine, Gerson, Gomez, Iagulli, Kuperberg, Lockaby, Mair, Mason, Mcpherson, Naclerio, Newcomb, Parker, Partland, Lamarkis Robinson, Nick Robinson, Romeo, Rozzo, Rushing, Senn, Simmons, Singh, Stinson, Szenkman, Traugott, Walts, Dolly Wright, Brittany Young, and Zenon (“Florida Plaintiffs”) also seek certification of the following state subclass (“Florida Subclass”):

All persons residing in Florida whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

329. Plaintiffs Box, Alisha Campbell, Caruthers, Chisum, Connuck, Cooper, Dowdell, Fears, Huddleston, Level, Jahmelia Lewis, Lowry, Maberry, Overton-Smith, Pettiford, Stiller, and Viggiano (“Georgia Plaintiffs”) also seek certification of the following state subclass (“Georgia

Subclass”):

All persons residing in Georgia whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

330. Plaintiff Murai (“Hawaii Plaintiff”) also seeks certification of the following state subclass (“Hawaii Subclass”):

All persons residing in Hawaii whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

331. Plaintiffs Bloom, Brady Collins, Kevin Collins, Kimberly Davis, Flesch, Gilmour, Mallon, Pry, Rosch, and Wilkerson (“Illinois Plaintiffs”) also seek certification of the following state subclass (“Illinois Subclass”):

All persons residing in Illinois whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

332. Plaintiffs Bass, Barbara Brooks, and Rodriguez (“Indiana Plaintiffs”) also seek certification of the following state subclass (“Indiana Subclass”):

All persons residing in Indiana whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

333. Plaintiffs Fredrickson, and Olive-Miller (“Iowa Plaintiff”) also seek certification of the following state subclass (“Iowa Subclass”):

All persons residing in Iowa whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

334. Plaintiffs Chasity Jackson, and Korn (“Kansas Plaintiffs”) also seek certification of the following state subclass (“Kansas Subclass”):

All persons residing in Kansas whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

335. Plaintiff Copeland (“Kentucky Plaintiff”) also seeks certification of the following

state subclass (“Kentucky Subclass”):

All persons residing in Kentucky whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

336. Plaintiffs Castle, Lapene, and Melissa Taylor (“Louisiana Plaintiffs”) also seek certification of the following state subclass (“Louisiana Subclass”):

All persons residing in Louisiana whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

337. Plaintiffs Bascom, Boston, Carol Cook, Coombs, Currie, Friedman, Christina Jackson, Perrier, and Robertson (“Maryland Plaintiffs”) also seek certification of the following state subclass (the “Maryland Subclass”):

All persons residing in Maryland whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

338. Plaintiffs Barrett, Dane, Kubinski, Masucci, Poltrack, and Preston (“Massachusetts Plaintiffs”) also seek certification of the following state subclass (“Massachusetts Subclass”):

All persons residing in Massachusetts whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

339. Plaintiffs Berrahou, Dorothy Brooks, Shanti Davis, Thomas Hickner, Hollingsworth, Lewandowski, Patton, Powell, Ruhlman, Shah, Gerald Taylor, Truskowski, and Wallace (“Michigan Plaintiffs”) also seek certification of the following state subclass (“Michigan Subclass”):

All persons residing in Michigan whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

340. Plaintiffs Carlisle, Keil, and Plank (“Minnesota Plaintiffs”) also seek certification of the following state subclass (“Minnesota Subclass”):

All persons residing in Minnesota whose Personal Information was

compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

341. Plaintiffs Betty Dampier, Draper, Miller, Rush, and Stigall (“Mississippi Plaintiffs”) also seek certification of the following state subclass (“Mississippi Subclass”):

All persons residing in Mississippi whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

342. Plaintiffs Covington, Haskett, Mankell, Ortner, and Simonitsch (“Missouri Plaintiffs”) also seek certification of the following state subclass (“Missouri Subclass”):

All persons residing in Missouri whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

343. Plaintiff Randolph White (“Montana Plaintiff”) also seeks certification of the following state subclass (“Montana Subclass”):

All persons residing in Montana whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

344. Plaintiff Tanika Moore (“Nebraska Plaintiff”) also seeks certification of the following state subclass (“Nebraska Subclass”):

All persons residing in Nebraska whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

345. Plaintiff Butler-Adams (“Nevada Plaintiff”) also seeks certification of the following state subclass (“Nevada Subclass”):

All persons residing in Nevada whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

346. Plaintiffs Bodie-Papino, Campanella, Andrew Hickner, Lizewska, Meade, Alicia Page, Shtofmakher, and Siandre (“New Jersey Plaintiffs”) also seek certification of the following state subclass (“New Jersey Subclass”):

All persons residing in New Jersey whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

347. Plaintiffs Betit, Cheng, Delaney, Diefenbach, Arnold Fishon, Eric Fishon, Forger, Galasso, Gupta, Hariaczyi, Moy, Nolan, Regne, and Ryan (“New York Plaintiffs”) also seek certification of the following state subclass (“New York Subclass”):

All persons residing in New York whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

348. Plaintiffs Juliet Black, Blackwell, Bovair, Meghan Cook, Desantis, Dudley, Eells, Shana Jordan, Gabrielle Moore, Murphy, Pageau, Pouliot, and Rowland (“North Carolina Plaintiffs”) also seek certification of the following state subclass (the “North Carolina Subclass”):

All persons residing in North Carolina whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

349. Plaintiffs Dubitsky, Johnson, Lear, Messer, Schmidt, Smallwood, Theiss, and Varner (“Ohio Plaintiffs”) also seek certification of the following state subclass (“Ohio Subclass”):

All persons residing in Ohio whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

350. Plaintiff Perkins (“Oklahoma Plaintiff”) also seeks certification of the following state subclass (“Oklahoma Subclass”):

All persons residing in Oklahoma whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

351. Plaintiff Cox (“Oregon Plaintiff”) also seeks certification of the following state subclass (“Oregon Subclass”):

All persons residing in Oregon whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

352. Plaintiffs Chieke, Davidez Dampier, Demarco, Teisha Jordan, Kern, Muick, Musto,

Rodgers, Spagnolo, and Springer (“Pennsylvania Plaintiffs”) also seek certification of the following state subclass (“Pennsylvania Subclass”):

All persons residing in Pennsylvania whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

353. Plaintiffs Callahan, Messier, and Matthew White (“Rhode Island Plaintiffs”) also seek certification of the following state subclass (“Rhode Island Subclass”):

All persons residing in Rhode Island whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

354. Plaintiffs Boykin, Gibbs, Ohara, Riggins, Sawyer, and Turnauer (“South Carolina Plaintiffs”) also seek certification of the following state subclass (“South Carolina Subclass”):

All persons residing in South Carolina whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

355. Plaintiffs Brown, Maxine Glass, Jennings, Tragarz, and Chris Wright (“Tennessee Plaintiffs”) also seek certification of the following state subclass (“Tennessee Subclass”):

All persons residing in Tennessee whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

356. Plaintiffs Cayla Campbell, Capper, Chism, Ciavarra, James Cook, Julie Davis, Dugat, Fanyui, Garden, Gardner, Hasan, Tameka Jackson, Kerkvliet, Tishaunda Lewis, Limen, Pfannenstiel, Ramirez, Sanderson, Spain, Stolte, Sykes, Theriot, Thompson, Vitasek, Clara White, and Wu (“Texas Plaintiffs”) also seek certification of the following state subclass (“Texas Subclass”):

All persons residing in Texas whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

357. Plaintiffs Abdulmalik, Darrell Black, Forrest, Lawler, Courtney Lewis, Valerie Lewis, and Ruga (“Virginia Plaintiffs”) also seek certification of the following state subclass (the

“Virginia Subclass”):

All persons residing in Virginia whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

358. Plaintiffs Duff, Hunter, Martin, and Risinger (“Washington Plaintiffs”) also seek certification of the following state subclass (the “Washington Subclass”):

All persons residing in Washington whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

359. Plaintiff Marco (“West Virginia Plaintiff”) also seek certification of the following state subclass (the “West Virginia Subclass”):

All persons residing in West Virginia whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

360. Plaintiffs Fornal and Mantei (“Wisconsin Plaintiffs”) also seek certification of the following state subclass (the “Wisconsin Subclass”):

All persons residing in Wisconsin whose Personal Information was compromised as a result of the data breach disclosed by Marriott on November 30, 2018.

361. The Class and Subclasses specifically exclude: (a) any persons or other entity currently related to or affiliated with Marriott; (b) any Judge presiding over this action and members of his or her family; and (c) all persons who properly execute and file a timely request for exclusion.

362. Class-wide adjudication of Plaintiffs’ claims is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

363. *Numerosity*: The members of the putative Class, estimated at 500 million, are so numerous that joinder of individual claims is impracticable. Members of the Class can be readily identified through Marriott’s records.

364. *Commonality*: There are significant questions of fact and law common to the members of the Class. These issues include but are not limited to:

- a. Whether Marriott failed to establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records to protect against known and anticipated threats to security;
- b. Whether Marriott failed to maintain adequate data security policies, procedures, and practices to secure Plaintiffs' and Class Members' PII;
- c. Whether the security provided by Marriott was satisfactory to protect customer information as compared to industry standards;
- d. Whether Marriott misrepresented or failed to provide adequate information to customers regarding the type of security practices used;
- e. Whether Marriott's conduct was intentional, willful or negligent;
- f. Whether Marriott violated any and all statutes and/or common law listed herein;
- g. Whether the putative Class suffered damages as a result of Marriott's conduct or omissions; and
- h. Whether Class Members are entitled to injunctive, declarative and monetary relief as a result of Marriott's conduct.

365. *Typicality*: Plaintiffs' claims are typical of the claims of the putative Class. Plaintiffs and all members of the putative Class have been adversely affected and damaged in that Marriott failed to adequately protect their PII to the detriment of Plaintiffs and the putative Class.

366. *Adequacy of Representation*: Plaintiffs, as the proposed Class Representatives, will fairly and adequately represent the putative Class because they have the Class Members' best interest in mind, because their individual claims are co-extensive with those of the Class, and because they are represented by qualified counsel experienced in class action litigation of this

nature.

367. *Superiority*: A class action in this instance is superior to other available methods for the fair and efficient adjudication of these claims because individual joinder of the claims of all members of the putative Class is impracticable. Many members of the Class are without the financial resources necessary to pursue this matter. Even if some members of the Class could afford to litigate their claims separately, such a result would be unduly burdensome to the courts in which the individualized cases would proceed. Individual litigation increases the time and expense of resolving a common dispute concerning Marriott's actions toward an entire group of individuals. Class action procedures allow for far fewer management difficulties in matters of this type and provide the unique benefits of unitary adjudication, economies of scale and comprehensive supervision over the entire controversy by a single judge in a single court.

368. The putative Class may be certified pursuant to Rule 23(b)(2) of the Federal Rules of Civil Procedure because Marriott has acted on grounds generally applicable to the putative Class, thereby making final injunctive relief and corresponding declaratory relief appropriate with respect to the claims raised by the Class.

369. The putative Class may also be certified pursuant to Rule 23(b)(3) of the Federal Rules of Civil Procedure because questions of law and fact common to Class Members will predominate over questions affecting individual members, and a class action is superior to other methods for fairly and efficiently adjudicating the controversy and causes of action described in this Complaint.

CLAIMS BROUGHT ON BEHALF OF NATIONWIDE CLASS

COUNT 1

BREACH OF IMPLIED CONTRACT

370. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

371. Marriott solicited and invited Plaintiffs and the members of the Class to make

reservations with Marriott. Plaintiffs and Class Members accepted Marriott's offers and made such reservations with Marriott.

372. When Plaintiffs and the Class made reservations with Marriott, they were required to, and did, provide their PII to Marriott. In so doing, Plaintiffs and Class Members entered into implied contracts with Marriott pursuant to which Marriott agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised.

373. Each reservation by Plaintiffs and Class Members was made pursuant to the mutually agreed-upon implied contract with Marriott under which Marriott agreed to safeguard and protect Plaintiffs' and Class Members' PII and to timely and accurately notify them if such information was compromised or stolen.

374. Plaintiffs and Class Members would not have provided and entrusted their PII to Marriott in the absence of the implied contract.

375. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Marriott.

376. Marriott breached the implied contracts they made with Plaintiffs and Class Members by failing to safeguard and protect the PII of Plaintiffs and Class Members and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the data breach.

377. As a direct and proximate result of Marriott's breaches of the implied contracts between Marriott and Plaintiffs and Class Members, Plaintiffs and Class Members sustained actual losses and damages as described in detail above.

COUNT 2

NEGLIGENCE

378. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

379. Upon accepting Plaintiffs' and Class Members' PII in its system, Marriott undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties, and to utilize commercially reasonable methods to do so. This duty included, among other things, designing, maintaining, and testing Marriott's security systems to ensure that Plaintiffs' and the Class Members' PII was adequately secured and protected, and to establish adequate data security policies, procedures, and practices to securely maintain Plaintiffs' and Class Members' PII.

380. Marriott further had a duty to implement processes that would detect a breach of their security systems in a timely manner and to timely act upon warnings and alerts, including those generated by their own security systems.

381. Marriott owed a duty to Plaintiffs and the Class to provide security consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the personal and financial information of Plaintiffs and Class Members.

382. Marriott knew, or should have known, of the risks inherent in collecting and storing the personal and financial information of Plaintiffs and the Class Members and of the critical importance of providing adequate security of that information.

383. Marriott breached the duties it owed to Plaintiffs and Class Members by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the personal and financial information of Plaintiffs and the Class.

384. Marriott breached the duties it owed to Plaintiffs and the Class by failing to properly implement technical systems or security policies, procedures, and practices that could have prevented the loss of the data at issue.

385. Marriott had a duty to timely disclose to Plaintiffs and the Class that their PII had

been or was reasonably believed to have been compromised. Timely disclosure was appropriate so that, among other things, Plaintiffs and the Class could take appropriate measures to avoid use of bank funds and monitor their account information and credit reports for fraudulent activity.

386. Marriott's failure to comply with its legal obligations and with industry standards and regulations, and the delay between the date of intrusion and the date Marriott disclosed the data breach, further evidences Marriott's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' personal and financial information in Marriott's possession.

387. Marriott knew that Plaintiffs and Class Members were foreseeable victims of a data breach of its system because of laws and statutes that require Marriott to reasonably safeguard sensitive payment information.

388. But for Marriott's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their personal and financial information would not have been compromised.

389. The injury and harm suffered by Plaintiffs and members of the Class as set forth above was the reasonably foreseeable result of Marriott's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' personal and financial information within Marriott's possession. Marriott knew or should have known that its systems and technologies for processing, securing, safeguarding and deleting Plaintiffs' and Class Members' personal and financial information were inadequate and vulnerable to being breached by hackers.

390. Plaintiffs and Class Members suffered injuries and losses described herein as a direct and proximate result of Marriott's conduct resulting in the data breach, including Marriott's lack of adequate reasonable and industry standard security measures. Had Marriott implemented such adequate and reasonable security measures, Plaintiffs and Class Members would not have suffered the injuries alleged, as the data breach would likely have not occurred.

391. As a direct and proximate result of Marriott's negligent conduct, Plaintiffs and the

Class have suffered injury and the significant risk of harm in the future, and are entitled to damages in an amount to be proven at trial.

392. Marriott breached its duty to discover and to notify Plaintiffs and the Class of the unauthorized access by failing to discover the security breach within reasonable time and by failing to notify Plaintiffs and Class Members of the breach until November 2018. To date, Marriott has not provided sufficient information to Plaintiffs and the Class regarding the extent and scope of the unauthorized access and Marriott continues to breach their disclosure obligations to Plaintiffs and the Class.

393. Marriott also breached its duty to Plaintiffs and Class Members to adequately protect and safeguard this information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering its negligent practices, Marriott failed to provide adequate supervision and oversight of the PII, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a third party to gather Plaintiffs' and Class Members' PII, misuse the PII, and intentionally disclose it to others without consent.

394. Through Marriott's acts and omissions described in this Complaint, including Marriott's failure to provide adequate security and its failure to protect Plaintiffs' and Class' PII from being foreseeably captured, accessed, disseminated, stolen, and misused, Marriott unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and Class' PII during the time it was within Marriott's control.

395. Further, through their failure to timely discover and provide clear notification of the data breach to consumers, Marriott prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PII.

396. Upon information and belief, Marriott improperly and inadequately safeguarded the PII of Plaintiffs and Class Members that deviated from standard industry rules, regulations, and

practices at the time of the data breach.

397. Neither Plaintiffs nor Class Members contributed to the Breach and subsequent misuse of their PII as described in this Complaint. As a direct and proximate result of Marriott's negligence, Plaintiffs and the Class sustained actual losses and damages as described in detail above.

COUNT 3

MARYLAND PERSONAL INFORMATION PROTECTION ACT

Md. Comm. Code §§ 14-3501, et seq.

398. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

399. Under Md. Comm. Code § 14-3503(a), “[t]o protect Personal Information from unauthorized access, use, modification, or disclosure, a business that owns or licenses Personal Information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of Personal Information owned or licensed and the nature and size of the business and its operations.”

400. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Md. Comm. Code §§ 14-3501(b)(1) and (2).

401. Plaintiffs and Class Members are “individuals” and “customers” as defined and covered by Md. Comm. Code §§ 14-3502(a) and 14-3503.

402. Plaintiffs’ and Class Members’ Private Information, as described herein and throughout, includes Personal Information as covered under Md. Comm. Code § 14-3501(d).

403. Marriott did not maintain reasonable security procedures and practices appropriate to the nature of the Personal Information owned or licensed and the nature and size of its business and operations in violation of Md. Comm. Code § 14-3503.

404. The Breach was a “breach of the security of a system” as defined by Md. Comm. Code § 14-3504(1).

405. Under Md. Comm. Code § 14-3504(b)(1), “[a] business that owns or licenses computerized data that includes Personal Information of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that Personal Information of the individual has been or will be misused as a result of the breach.”

406. Under Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), “[i]f, after the investigation is concluded, the business determines that misuse of the individual’s Personal Information has occurred or is reasonably likely to occur as a result of a breach of the security system, the business shall notify the individual of the breach” and that notification “shall be given as soon as reasonably practical after the business discovers or is notified of the breach of a security system.”

407. Because Marriott discovered a security breach and had notice of a security breach, Marriott had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

408. By failing to disclose the Breach in a timely and accurate manner, Marriott violated Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

409. As a direct and proximate result of Marriott’s violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), Plaintiffs and Class Members suffered damages, as described above.

410. Pursuant to Md. Comm. Code § 14-3508, Marriott’s violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of the Maryland Consumer Protection Act, 13 Md. Comm. Code §§ 13-101, et seq. and subject to the enforcement and penalty provisions contained within the Maryland Consumer Protection Act.

411. Plaintiffs and Class Members seek relief under Md. Comm. Code §13-408, including actual damages and attorney’s fees.

COUNT 4

MARYLAND CONSUMER PROTECTION ACT

Md. Comm. Code §§ 13-301, et seq.

412. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.
413. Defendants are a “persons” as defined by Md. Comm. Code § 13-101(h).
414. Marriott’s conduct as alleged herein related to “sales,” “offers for sale,” or “bailment” as defined by Md. Comm. Code § 13-101(i) and § 13-303.
415. Plaintiffs and Class Members are “consumers” as defined by Md. Comm. Code § 13-101(c).
416. Marriott advertises, offers, or sells “consumer goods” or “consumer services” as defined by Md. Comm. Code § 13-101(d).
417. Marriott advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland.
418. Marriott engaged in unfair and deceptive trade practices, in violation of Md. Comm. Code § 13-301, including:
- a. False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;
 - b. Failing to state a material fact where the failure deceives or tends to deceive;
 - c. Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered;
 - d. Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale lease or rental.
419. Marriott engaged in these unfair and deceptive trade practices in connection with

offering for sale or selling consumer goods or services or with respect to the extension of consumer credit, in violation of Md. Comm. Code § 13-303, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' personal and confidential information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' personal and confidential information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503, which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' personal and confidential information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Comm. Code § 14- 3503;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and

the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503.

420. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' personal and confidential information. Marriott's misrepresentations and omissions would have been important to a significant number of consumers in making financial decisions.

421. Marriott intended to mislead Plaintiffs and Class Members and induce them to rely on their misrepresentations and omissions.

422. Had Marriott disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been forced to adopt reasonable data security measures and comply with the law.

423. Marriott acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded Plaintiffs' and Class Members' rights.

424. Marriott was on notice of the possibility of the Data Breach due to its prior data breach and infiltrations of its systems in the past.

425. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

426. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

COUNT 5

BAILMENT

427. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

428. Plaintiffs and Class Members provided, or authorized disclosure of, their PII to Marriott for the exclusive purpose of booking hotel reservations and/or airline travel.

429. In allowing their personal and financial information to be made available to Marriott, Plaintiffs and Class Members intended and understood that Marriott would adequately safeguard their personal and financial information.

430. Marriott accepted possession of Plaintiffs' and Class Members' personal and financial information for the purpose of making available to Plaintiffs and Class Members Marriott's services for their benefit.

431. By accepting possession of Plaintiffs' and Class Members' personal and financial information, Marriott understood that Plaintiffs and Class Members expected Marriott to adequately safeguard their personal and financial information. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties. During the bailment (or deposit), Marriott owed a duty to Plaintiffs and Class Members to exercise reasonable care, diligence, and prudence in protecting their personal and financial information.

432. Marriott breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and Class Members' personal and financial information, resulting in the unlawful and unauthorized access to and misuse of Plaintiffs' and Class Members' personal and financial information.

433. Marriott further breached its duty to safeguard Plaintiffs' and Class Members' personal and financial information by failing to timely and accurately discover the breach and by failing to timely and accurately notify them that their information had been compromised as a result of the data breach.

434. As a direct and proximate result of Marriott's breach of its duty, Plaintiffs and Class Members suffered consequential damages that were reasonably foreseeable to Marriott, including but not limited to the damages set forth above.

435. As a direct and proximate result of Marriott's breach of its duty, the personal and financial information of Plaintiffs and Class Members entrusted, directly or indirectly, to Marriott during the bailment (or deposit) was damaged and its value diminished.

COUNT 6

NEGLIGENCE PER SE

436. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

437. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Marriott had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

438. Pursuant to state laws in at least the following 13 states, Marriott had a duty to those respective states' Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' Personal Information:

- a. Arkansas: Ark. Code § 4-110-104
- b. California: Cal Civ. Code § 1798.81.5
- c. Connecticut: Conn. Gen. Stat. § 42-471
- d. Florida: Fla. Stat. § 501.171(2)
- e. Georgia: Ga. Code Ann., § 10-1-912
- f. Indiana: Ind. Code § 24-4.9-3.5
- g. Maryland: Md. Code. Comm. Law § 14-5303
- h. Massachusetts: Mass. Gen Laws Ch. 93H, § 3(a)
- i. Nevada: Nev. Rev. Stat. § 603A.210
- j. Oregon: Ore. Rev. Stat. § 646A.622(1)

k Rhode Island: R.I. Gen Laws § 11-49.2-2(2)

l Texas: Tex. Bus. & Com. Code § 521.052(a) m.

m Utah: Utah Code § 14-44-201(1)(a)

439. Marriott breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45) and the state data security statutes by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Personal Information.

440. Marriott's failure to comply with applicable laws and regulations constitutes negligence per se.

441. But for Marriott's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

442. The injury and harm suffered by Plaintiffs and the Class Members was the reasonably foreseeable result of Marriott's breach of their duties. Marriott knew or should have known that they were failing to meet their duties, and that the breach would cause Plaintiffs and the State Class Members to experience the foreseeable harms associated with the exposure of their PII.

443. As a direct and proximate result of Marriott's negligent conduct, Plaintiffs and the Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT 7

BREACH OF DUTY OF GOOD FAITH AND FAIR DEALING

444. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

445. The law implies a covenant of good faith and fair dealing in every contract.

446. Plaintiffs and Class Members contracted with Marriott by accepting Marriott's offers to stay at one or more of its hotels.

447. Plaintiffs and Class Members performed all of the significant duties under their

agreements with Marriott.

448. The conditions required for Marriott's performance under the contract has occurred.

449. Marriott did not provide and/or unfairly interfered with and/or frustrated the right of Plaintiffs and the Class Members to receive the full benefits under their agreement.

450. Marriott breached the covenant of good faith and fair dealing implied in its contracts with Plaintiffs and the Class Members by failing to use and provide reasonable and industry-leading security practices to protect Plaintiffs' and the Class Members' PII.

451. Plaintiffs and the Class Members were damaged by Marriott's breach in that they paid for, but never received, the valuable security protections to which they were entitled, and which would have made their products and services more valuable.

COUNT 8

INVASION OF PRIVACY

452. Plaintiffs and the Class Members incorporate by reference each preceding paragraph as though fully set forth at length herein.

453. Marriott invaded Plaintiffs' and the Class Members' right to privacy by allowing the unauthorized access to Plaintiffs' and Class Members' PII and by negligently maintaining the confidentiality of Plaintiffs' and Class Members' PII, as set forth above.

454. The intrusion was offensive and objectionable to Plaintiffs, the Class Members, and to a reasonable person of ordinary sensibilities in that Plaintiffs' and Class Members' PII was disclosed without prior written authorization of Plaintiffs and the Class.

455. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiffs' and the Class Members provided and disclosed their PII to Marriott privately with an intention that the PII would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class Members were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

456. As a proximate result of Marriott's above acts, Plaintiffs' and the Class Members' PII was viewed, printed, distributed, and used by persons without prior written authorization and Plaintiff and the Class Members suffered damages.

457. Marriott committed oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiffs' and the Class Members' PII with a willful and conscious disregard of Plaintiffs' and the Class Members' right to privacy.

458. Unless and until enjoined, and restrained by order of this Court, Marriott's wrongful conduct will continue to cause Plaintiffs and the Class Members great and irreparable injury in that the PII maintained by Marriott can be viewed, printed, distributed, and used by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

COUNT 9

DECLARATORY RELIEF

459. Plaintiffs and the Class Members incorporate by reference each preceding paragraph as though fully set forth at length herein.

460. Pursuant to the Declaratory Judgment Act, 28 U.S.C. §2201, *et seq.*; Fed. R. Civ. P. 57, Plaintiffs and Class Members request the Court to enter a judgment declaring, *inter alia*, (i) Marriott owed (and continues to owe) a legal duty to safeguard and protect Plaintiffs' and Class Members' PII, and timely notify them about any security breach, (ii) Marriott breached (and continues to breach) such legal duties by failing to safeguard and protect Plaintiffs' and Class Members' PII, and (iii) Marriott's breach of its legal duties directly and proximately caused the security breach, and the resulting damages, injury, and harm suffered by Plaintiffs and Class Members.

COUNT 10

INJUNCTIVE RELIEF

461. Plaintiffs and the Class Members incorporate by reference each preceding paragraph as though fully set forth at length herein.

462. Marriott's above-described wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and the resulting security breach have caused (and will continue to cause) Plaintiffs and Class Members to suffer irreparable harm in the form of, *inter alia*, economic damages and other injury and actual harm in the form of, *inter alia*, (i) actual identity theft and identity fraud, (ii) invasion of privacy, (iii) loss of the intrinsic value of their privacy, (iv) breach of the confidentiality of their consumer reports and consumer credit information, (v) deprivation of the value of their consumer credit information, for which there is a well- established national and international market, (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages, and (vii) the imminent, immediate, and continuing increased risk of ongoing identity theft and identity fraud. Such irreparable harm will not cease unless and until enjoined by this Court.

463. Plaintiffs and Class Members, therefore, are entitled to injunctive relief and other appropriate affirmative relief including, *inter alia*, an order compelling Marriott to, *inter alia*, (i) notify each person whose consumer credit information was exposed in the security breach, (ii) provide credit monitoring to each such person for at least six years, (iii) establish a fund (in an amount to be determined) to which such persons may apply for reimbursement of the time and out-of-pocket expenses they incurred to remediate identity theft and/or identity fraud (*i.e.*, data breach insurance), and (iv) discontinue its above-described wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and the resulting security breach.

464. Plaintiffs and Class Members also are entitled to injunctive relief requiring Marriott to implement and maintain data security measures, policies, procedures, controls,

protocols, and software and hardware systems, including, *inter alia*, (i) engaging third-party security auditors/penetration testers and internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Marriott's computer systems on a periodic basis, (ii) engaging third-party security auditors and internal personnel to run automated security monitoring, (iii) auditing, testing, and training its security personnel regarding any new or modified procedures, (iv) conducting regular database scanning and security checks, (v) regularly evaluating web applications for vulnerabilities to prevent web application threats, and (vi) periodically conducting internal training and education to inform internal data security personnel how to identify and contain data security lapses.

465. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury in the event Marriott commits another security lapse, the risk of which is real, immediate, and substantial.

466. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Marriott if an injunction is issued. Among other things, if Marriott suffers another massive security lapse, Plaintiffs and Class Members will likely again incur millions of dollars in damages. On the other hand, and setting aside the fact that Marriott have a pre-existing legal obligation to employ adequate customer data security measures, Marriott's cost to comply with the above-described injunction they are already required to implement is relatively minimal.

467. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another security lapse, thereby eliminating the damages, injury, and harm that would be suffered by Plaintiffs, Class Members, and the millions of consumers whose confidential and sensitive consumer credit information would be compromised.

CLAIMS ON BEHALF OF THE ALABAMA SUBCLASS

COUNT 11

ALABAMA DECEPTIVE TRADE PRACTICES ACT

Ala. Code §§ 8-19-1, et seq.

468. Alabama Plaintiffs identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the Alabama Subclass, repeats and alleges all previous Paragraphs as if fully alleged herein.

469. Marriott is a “person” as defined by Ala. Code § 8-19-3(5).

470. Plaintiffs and Alabama Subclass members are “consumers” as defined by Ala. Code § 8-19-3(2).

471. Plaintiffs sent pre-suit notice pursuant to Ala. Code § 8-19-10(e) on December 11, 2018.

472. Marriott advertised, offered, or sold goods or services in Alabama, and engaged in trade or commerce directly or indirectly affecting the people of Alabama.

473. Marriott engaged in deceptive acts and practices in the conduct of trade or commerce, in violation of the Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5, including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and

c. Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce, including acts and practices that would violate Section 5(a)(1) of the FTC Act, as interpreted by the FTC and federal courts.

474. Marriott’s deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Alabama Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Alabama Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Alabama Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alabama Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Alabama Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Alabama Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

475. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect

the confidentiality of consumers' Personal Information.

476. Marriott intended to mislead Plaintiffs and Alabama Subclass members and induce them to rely on its misrepresentations and omissions.

477. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

478. Marriott accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public. Accordingly, because Marriott held itself out as being trustworthy and secure, Plaintiffs and the Alabama Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

479. Marriott acted intentionally, knowingly, and maliciously to violate the Alabama Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Alabama Subclass members' rights. past data breaches put it on notice that its security and privacy protections were inadequate.

480. As a direct and proximate result of Marriott's deceptive acts and practices, Plaintiffs and Alabama Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

481. Marriott's deceptive acts and practices caused substantial injury to Plaintiffs and Alabama Subclass members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

482. Plaintiffs and the Alabama Subclass seek all monetary and nonmonetary relief allowed by law, including the greater of (a) actual damages or (b) statutory damages of \$100; treble damages; injunctive relief; attorneys' fees, costs, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE ARIZONA SUBCLASS

COUNT 12

ARIZONA CONSUMER FRAUD ACT

A.R.S. §§ 44-1521, et seq.

483. Arizona Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Arizona Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

484. Marriott is a "person" as defined by A.R.S. § 44-1521(6).

485. Marriott advertised, offered, or sold goods or services in Arizona and engaged in trade or commerce directly or indirectly affecting the people of Arizona.

486. Marriott engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts affecting the people of Arizona in connection with the sale and advertisement of "merchandise" (as defined in Arizona Consumer Fraud Act, A.R.S. § 44-1521(5)) in violation of A.R.S. § 44-1522(A), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Arizona Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Arizona Subclass members' Personal Information, including

duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Arizona Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Arizona Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Arizona Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Arizona Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

487. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

488. Marriott intended to mislead Plaintiffs and Arizona Subclass members and induce them to rely on its misrepresentations and omissions.

489. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as trustworthy and secure.

490. Marriott accepted the responsibility of being a "steward of data" while keeping the

inadequate state of its security controls secret from the public.

491. Plaintiffs and the Arizona Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

492. Marriott acted intentionally, knowingly, and maliciously to violate Arizona's Consumer Fraud Act, and recklessly disregarded Plaintiffs and Arizona Subclass members' rights. Past breaches put it on notice that its security and privacy protections were inadequate.

493. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiffs and Arizona Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

494. Plaintiffs and Arizona Subclass members seek all monetary and nonmonetary relief allowed by law, including compensatory damages; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE ARKANSAS SUBCLASS

COUNT 13

ARKANSAS DECEPTIVE TRADE PRACTICES ACT

A.C.A. §§ 4-88-101, et seq.

495. Arkansas Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Arkansas Subclass, repeat and alleges all previous Paragraphs, as if fully alleged herein.

496. Marriott is a "person" as defined by A.C.A. § 4-88-102(5).

497. Marriott's products and services are "goods" and "services" as defined by A.C.A. §§ 4-88-102(4) and (7).

498. Marriott advertised, offered, or sold goods or services in Arkansas and engaged in trade or commerce directly or indirectly affecting the people of Arkansas.

499. The Arkansas Deceptive Trade Practices Act (“ADTPA”), A.C.A. §§ 4-88-101, et seq., prohibits unfair, deceptive, false, and unconscionable trade practices.

500. Marriott engaged in acts of deception and false pretense in connection with the sale and advertisement of services in violation of A.C.A. § 4-88-1-8(1) and concealment, suppression and omission of material facts, with intent that others rely upon the concealment, suppression or omission in violation of A.C.A. § 4-88-1-8(2), and engaged in the following deceptive and unconscionable trade practices defined in A.C.A. § 4-88-107:

- a. Knowingly making a false representation as to the characteristics, ingredients, uses, benefits, alterations, source, sponsorship, approval, or certification of goods or services and as to goods being of a particular standard, quality, grade, style, or model;

- b. Advertising goods or services with the intent not to sell them as advertised;

- c. Employing consistent bait-and-switch advertising of an attractive but insincere offer to sell a product or service which the seller in truth does not intend or desire to sell, as evidenced by acts demonstrating an intent not to sell the advertised product or services;

- d. Knowingly taking advantage of a consumer who is reasonably unable to protect his or her interest because of ignorance; and

- e. Engaging in other unconscionable, false, or deceptive acts and practices in business, commerce, or trade.

501. Marriott’s unconscionable, false, and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Arkansas Subclass members’ Personal Information, which was a direct and proximate cause of the Breach;

- b. Failing to identify foreseeable security and privacy risks, remediate

identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Arkansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Arkansas Personal Information Protection Act, A.C.A. § 4-110-104(b), which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Arkansas Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Arkansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Arkansas Personal Information Protection Act, A.C.A. § 4-110-104(b);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Arkansas Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Arkansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Arkansas Personal Information Protection Act, A.C.A. § 4-110-104(b).

502. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

503. Marriott intended to mislead Plaintiffs and Arkansas Subclass members and induce them to rely on its misrepresentations and omissions.

504. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as trustworthy and secure.

505. Marriott accepted the responsibility of being a “steward of data” while keeping the inadequate state of its security controls secret from the public.

506. Plaintiffs and the Arkansas Subclass members acted reasonably in relying on Marriott’s misrepresentations and omissions, the truth of which they could not have discovered.

507. Marriott acted intentionally, knowingly, and maliciously to violate Arkansas’s Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs and Arkansas Subclass members’ rights. Past data breaches put it on notice that its security and privacy protections were inadequate.

508. As a direct and proximate result of Marriott’s unconscionable, unfair, and deceptive acts or practices and Plaintiffs and Arkansas Subclass members’ reliance thereon, Plaintiffs and Arkansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

509. Plaintiffs and the Arkansas Subclass members seek all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys’ fees and costs.

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT 14

CALIFORNIA CUSTOMER RECORDS ACT

Cal. Civ. Code §§ 1798.80, et seq.

510. California Plaintiffs identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the California Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

511. “[T]o ensure that Personal Information about California residents is protected,” the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that “owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure.”

512. Marriott is a business that owns, maintains, and licenses Personal Information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiffs and California Subclass members.

513. Businesses that own or license computerized data that includes Personal Information are required to notify California residents when their Personal Information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach “in the most expedient time possible and without unreasonable delay.” Cal. Civ. Code § 1798.82.

514. Among other requirements, the security breach notification must include “the types of Personal Information that were or are reasonably believed to have been the subject of the breach.” Cal. Civ. Code § 1798.82.

515. Marriott is a business that owns or licenses computerized data that includes

Personal Information as defined by Cal. Civ. Code § 1798.82.

516. Plaintiffs and California Subclass members' PII includes Personal Information as covered by Cal. Civ. Code § 1798.82.

517. Because Marriott reasonably believed that Plaintiffs' and California Subclass members' Personal Information was acquired by unauthorized persons during the Breach, Marriott had an obligation to disclose the Breach in a timely and accurate fashion as mandated by Cal. Civ. Code §1798.82.

518. By failing to disclose the Breach in a timely and accurate manner, Marriott violated Cal. Civ. Code § 1798.82.

519. As a direct and proximate result of Marriott's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiffs and California Subclass members suffered damages, as described above.

520. Plaintiffs and California Subclass members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT 15

CALIFORNIA UNFAIR COMPETITION LAW

Cal. Bus. & Prof. Code §§ 17200, et seq.

521. California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeats and all previous Paragraphs, as if fully alleged herein.

522. Marriott is a "person" as defined by Cal. Bus. & Prof. Code §17201.

523. Marriott violated Cal. Bus. & Prof. Code §§ 17200, et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

524. Marriott's "unfair" acts and practices include:

a. Marriott failed to implement and maintain reasonable security measures to

protect Plaintiffs and California Subclass members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Breach. Marriott failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiffs and the California Subclass, whose Personal Information has been compromised.

b. Marriott's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45) and California's Consumer Records Act (Cal. Civ. Code § 1798.81.5).

c. Marriott's failure to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Marriott's inadequate security, consumers could not have reasonably avoided the harms that Marriott caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

525. Marriott has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq., the FTC Act, 15 U.S.C. § 45, and California common law.

526. Marriott's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures

to protect Plaintiffs and California Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and California Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and California Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.

527. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect

the confidentiality of consumers' Personal Information.

528. As a direct and proximate result of Marriott's unfair, unlawful, and fraudulent acts and practices, Plaintiffs and California Subclass members were injured and lost money or property, including the costs passed through to Marriott from their consumer credit transactions, the premiums and/or price received by Marriott for its goods and services, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Personal Information.

529. Marriott acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs and California Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

530. Plaintiffs and California Subclass members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Marriott's unfair, unlawful, and fraudulent business practices or use of their Personal Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT 16

CALIFORNIA CONSUMER LEGAL REMEDIES ACT

Cal. Civ. Code §§ 1750, et seq.

531. California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

532. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, et seq. ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against

unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

533. Marriott is a “person” as defined by Civil Code §§ 1761(c) and 1770, and has provided “services” as defined by Civil Code §§ 1761(b) and 1770.

534. Plaintiffs and the California Class are “consumers” as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a “transaction” as defined by Civil Code §§ 1761(e) and 1770.

535. Marriott’s acts and practices were intended to and did result in the sales of products and services to Plaintiffs and the California Subclass members in violation of Civil Code § 1770, including:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade when they were not;
- c. Advertising goods or services with intent not to sell them as advertised; and
- d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

536. Marriott’s representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott’s data security and ability to protect the confidentiality of consumers’ Personal Information.

537. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as trustworthy and secure.

538. Marriott accepted the responsibility of being a “steward of data” while keeping the

inadequate state of its security controls secret from the public.

539. Plaintiffs and the California Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

540. As a direct and proximate result of Marriott's violations of California Civil Code § 1770, Plaintiffs and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

541. Plaintiffs and the California Subclass have provided notice of their claims for damages to Marriott, in compliance with California Civil Code § 1782(a).

542. Plaintiffs and the California Subclass seek all monetary and nonmonetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

CLAIMS ON BEHALF OF THE COLORADO SUBCLASS

COUNT 17

VIOLATION OF THE COLORADO CONSUMER PROTECTION ACT

Colo. Rev. Stat. § 6-1-101, et. seq.

543. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

544. Marriott, while operating in Colorado, engaged in deceptive practices in the course of its business, vocation, and occupation, in violation of C.R.S. §6-1-105. This includes, but is not limited to, the following:

a. Marriott failed to enact adequate privacy and security measures to protect the Colorado Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Marriott failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Marriott knowingly and fraudulently misrepresented that they would maintain adequate data privacy and security practices and procedures to safeguard Colorado Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, in violation of Colo. Rev. Stat. §6-1-105(e), (g) and (u);

d. Marriott knowingly and fraudulently misrepresented that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Colorado Subclass members' PII, in violation of Colo. Rev. Stat. §6-1-105(e), (g) and (u);

e. Marriott knowingly omitted, suppressed, and concealed the inadequacy of the privacy and security protections for Colorado Class members' PII, in violation of Colo. Rev. Stat. §6-1-105(1)(e), (g) and (u);

f. Marriott failed to maintain the privacy and security of Plaintiffs' and the Colorado Subclass members' PII, in violation of duties imposed by applicable federal and state laws, which was a direct and proximate cause of the Data Breach; and

g. Marriott failed to disclose the Data Breach to the Colorado Subclass members in a timely and accurate manner, in violation of the duties imposed by Colo. Rev. Stat. Ann § 6-1-716(2).

545. As a direct and proximate result of Marriott's practices, the Colorado Subclass members suffered injuries to legally protected interests, as described above, including their legally protected interest in the confidentiality and privacy of their PII, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII.

546. The above unfair and deceptive practices and acts by Marriott were immoral,

unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

547. Marriott knew or should have known that data security practices and infrastructure were inadequate to safeguard the PII of members of the Colorado Subclass, and that risk of a data breach or theft was highly likely. Marriott's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Colorado Subclass members.

548. Pursuant to Colo. Rev. Stat. § 6-1-113, Plaintiffs, individually and on behalf of the Colorado Subclass, seek monetary relief against Marriott measured as the greater of (a) actual damages in an amount to be determined at trial and discretionary trebling of such damages, or (b) statutory damages in the amount of \$500 for each Plaintiff and each Colorado Subclass member.

549. Plaintiffs also seek an order enjoining Marriott's unfair, unlawful, and/or deceptive practices, declaratory relief, attorneys' fees, and any other just and proper relief available under the Colorado Consumer Protection Act, Colo. Rev. Stat § 6-1-101, et seq.

COUNT 18

VIOLATION OF THE COLORADO SECURITY BREACH NOTIFICATION ACT

Colo. Rev. Stat. Ann. § 6-1-716, et. seq.

550. Plaintiffs incorporate by reference all paragraphs above as though fully set forth herein.

551. Under Colo. Rev. Stat. Ann. § 6-1-716(2)(a), "a commercial entity that conducts business in Colorado and that owns or licenses computerized data that includes personal information about a resident of Colorado shall, when it becomes aware of a breach of the security of the system, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused ... [and] give notice as soon as possible to the

affected Colorado resident”

552. Under Colo. Rev. Stat. Ann. § 6-1-716(2)(b), “a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach”

553. Marriott is a business that owns or licenses computerized data that includes personal information as defined by Colo. Rev. Stat. Ann. § 6-1-716.

554. In the alternative, Marriott maintains computerized data that includes personal information that Marriott does not own as defined by Colo. Rev. Stat. Ann. § 6-1-716.

555. Plaintiffs and the Colorado Subclass members’ PII includes personal information covered by Colo. Rev. Stat. Ann. § 6-1-716(1).

556. Because Marriott was aware of a breach in its security system, it had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. Ann. § 6-1-716 (2).

557. By failing to disclose the Data Breach in a timely and accurate manner, Marriott violated Colo. Rev. Stat. Ann. § 6-1-716 (2).

558. As a direct and proximate result of Marriott’s violations of Colo. Rev. Stat. Ann. § 6-1-716(2), Plaintiffs and the Colorado Subclass members suffered the damages alleged herein.

559. Plaintiffs and the Colorado Subclass members seek relief under Colo. Rev. Stat. Ann. § 6-1-716(4), including, but not limited to, actual damages (to be proven at trial) and equitable relief.

CLAIMS ON BEHALF OF THE CONNECTICUT SUBCLASS

COUNT 19

BREACH OF SECURITY REGARDING COMPUTERIZED DATA

C.G.S.A. § 36a-701b

560. Connecticut Plaintiffs identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the Connecticut Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

561. Marriott is a business that conducts business in Connecticut and owns, licenses, and maintains computerized data that includes personal information as covered by C.G.S.A. § 36a-701b(b). Marriott also maintains computerized data that includes personal information that it does not own as covered by C.G.S.A. § 36a-701b(c).

562. Plaintiffs and Connecticut Subclass members’ PII includes Personal Information as covered by C.G.S.A. § 36a-701b(a).

563. Marriott is required to accurately notify Plaintiffs and Connecticut Subclass members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay, not to exceed ninety days after discovery of the breach under C.G.S.A. § 36a-701b(b).

564. Marriott is required to immediately notify Plaintiffs and Connecticut Subclass members if it becomes aware of a breach of its data security system which may have compromised personal information Marriott stores but Plaintiffs and Connecticut Subclass members own under C.G.S.A. § 36a-701b(c).

565. Because Marriott was aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by C.G.S.A. §§ 36a-701b(b) and (c).

566. By failing to disclose the Breach in an accurate and timely manner, Marriott failed

to comply with C.G.S.A. §§ 36a-701b(b) and (c).

567. Pursuant to C.G.S.A. § 36a-701b(g), Marriott's failure to comply was an unfair trade practice under the Connecticut Unfair Trade Practices Act, C.G.S.A. §§ 42-110a, et seq.

568. As a direct and proximate result of Marriott's violations of C.G.S.A. §§ 36a-701b(b) and (c), Plaintiffs and Connecticut Subclass members suffered damages, as described above.

569. Plaintiffs and Connecticut Subclass members seek relief under C.G.S.A. § 42-110g for the harm they suffered because of Marriott's violations of C.G.S.A. §§ 36a-701b(b) and (c), including actual damages and equitable relief.

CLAIMS ON BEHALF OF THE DISTRICT OF COLUMBIA SUBCLASS

COUNT 20

DISTRICT OF COLUMBIA CONSUMER SECURITY BREACH NOTIFICATION ACT

D.C. Code §§ 28-3851, et seq.

570. District of Columbia Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the District of Columbia Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

571. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by D.C. Code § 28-3852(a).

572. Plaintiffs and District of Columbia Subclass members' PII includes Personal Information as covered under D.C. Code § 28-3851(3).

573. Marriott is required to accurately notify Plaintiffs and District of Columbia Subclass members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under D.C. Code § 28-3852(a).

574. Because Marriott was aware of a breach of its security system, Marriott had an obligation to disclose the data breach in a timely and accurate fashion as mandated by D.C. Code §

28-3852(a).

575. By failing to disclose the Breach in a timely and accurate manner Marriott violated D.C. Code § 28-3852(a).

576. As a direct and proximate result of Marriott's violations of D.C. Code § 28-3852(a), Plaintiffs and District of Columbia Subclass members suffered damages, as described above.

577. Plaintiffs and District of Columbia Subclass members seek relief under D.C. Code § 28-3853(a), including actual damages.

COUNT 21

DISTRICT OF COLUMBIA CONSUMER PROTECTION PROCEDURES ACT

D.C. Code §§ 28-3904, et seq.

578. District of Columbia Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the District of Columbia Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

579. Marriott is a "person" as defined by D.C. Code § 28-3901(a)(1).

580. Marriott is a "merchant" as defined by D.C. Code § 28-3901(a)(3).

581. Plaintiffs and District of Columbia Subclass members are "consumers" who purchased or received goods or services for personal, household, or family purposes, as defined by D.C. Code § 28-3901.

582. Marriott advertised, offered, or sold goods or services in District of Columbia and engaged in trade or commerce directly or indirectly affecting the people of District of Columbia.

583. Marriott engaged in unfair, unlawful, and deceptive trade practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods and services in violation of D.C. Code § 28-3904, including:

a. Representing that goods or services have characteristics that they do not

have;

b. Representing that goods or services are of a particular standard, quality, grade, style, or model, when they are of another;

c. Misrepresenting a material fact that has a tendency to mislead;

d. Failing to state a material fact where the failure is misleading;

e. Advertising or offering goods or services without the intent to sell them as advertised or offered; and

f. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

584. Marriott's unfair, unlawful, and deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and District of Columbia Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and District of Columbia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and District of Columbia Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and District of Columbia Subclass members'

Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and District of Columbia Subclass members' Personal Information; and

g Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and District of Columbia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

585. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

586. Marriott intended to mislead Plaintiffs and District of Columbia Subclass members and induce them to rely on its misrepresentations and omissions.

587. The above unfair and deceptive practices and acts by Marriott were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and District of Columbia Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

588. Marriott acted intentionally, knowingly, and maliciously to violate the District of Columbia's Consumer Protection Procedures Act, and recklessly disregarded Plaintiffs and District of Columbia Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

589. As a direct and proximate result of Marriott's unfair, unlawful, and deceptive trade practices, Plaintiffs and District of Columbia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial

accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

590. Plaintiffs and District of Columbia Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, injunctive relief, punitive damages, attorneys' fees and costs, the greater of treble damages or \$1500 per violation, and any other relief that the Court deems proper.

CLAIMS ON BEHALF OF THE DELAWARE SUBCLASS

COUNT 22

DELAWARE CONSUMER FRAUD ACT,

6 Del. Code §§ 2513, et seq.

591. Delaware Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Delaware Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

592. Marriott is a "person" that is involved in the "sale" of "merchandise," as defined by 6 Del. Code § 2511(7), (8), and (6).

593. Marriott advertised, offered, or sold goods or services in Delaware and engaged in trade or commerce directly or indirectly affecting the people of Delaware.

594. Marriott used and employed deception, fraud, false pretense, false promise, misrepresentation, and the concealment, suppression, and omission of material facts with intent that others rely upon such concealment, suppression and omission, in connection with the sale and advertisement of merchandise, in violation of 6 Del. Code § 2513(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Delaware Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate

identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Delaware Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Delaware's data security statute, 6 Del. Code § 12B-100, which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Delaware Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Delaware Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Delaware's data security statute, 6 Del. Code § 12B-100;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Delaware Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Delaware Subclass members' Personal Information, including duties imposed by FTC Act, 15 U.S.C. § 45 and Delaware's data security statute, 6 Del. Code § 12B-100.

595. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

596. Marriott acted intentionally, knowingly, and maliciously to violate Delaware's Consumer Fraud Act, and recklessly disregarded Plaintiff and Delaware Subclass members' rights.

Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

597. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as secure and was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Delaware Subclass.

598. Marriott accepted the responsibility of being a “steward of data” while keeping the inadequate state of its security controls secret from the public.

599. Plaintiff and the Delaware Subclass members acted reasonably in relying on Marriott’s misrepresentations and omissions, the truth of which they could not have discovered.

600. Marriott’s unlawful trade practices were gross, oppressive, and aggravated, and Marriott breached the trust of Plaintiff and the Delaware Subclass members.

601. As a direct and proximate result of Marriott’s unlawful acts and practices, Plaintiff and Delaware Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

602. Plaintiff and Delaware Subclass members seek all monetary and nonmonetary relief allowed by law, including damages under 6 Del. Code § 2525 for injury resulting from the direct and natural consequences of Marriott’s unlawful conduct; injunctive relief; and reasonable attorneys’ fees and costs.

CLAIMS ON BEHALF OF THE FLORIDA SUBCLASS

COUNT 23

FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT

Fla. Stat. §§ 501.201, et seq.

603. Florida Plaintiffs identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the Florida Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

604. Plaintiffs and Florida Subclass members are “consumers” as defined by Fla. Stat. § 501.203.

605. Marriott advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

606. Marriott engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Florida Subclass members’ Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Florida Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida’s data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Florida Subclass members’ Personal Information, including by implementing and

maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Florida's data security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Florida Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Florida's data security statute, F.S.A. § 501.171(2).

607. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

608. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as secure, and was Marriott was trusted with sensitive and valuable Personal Information regarding millions of consumers, including Plaintiff and the Florida Subclass.

609. Marriott accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public.

610. Plaintiffs and the Florida Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

611. As a direct and proximate result of Marriott's unconscionable, unfair, and deceptive acts and practices, Plaintiffs and Florida Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

612. Plaintiffs and Florida Subclass members seek all monetary and nonmonetary relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.21; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE GEORGIA SUBCLASS

COUNT 24

GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT

O.C.G.A. §§ 10-1-370, et seq.

613. Georgia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Georgia Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

614. Marriott, Plaintiff, and Georgia Subclass members are "persons" within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

615. Marriott engaged in deceptive trade practices in the conduct of its business, in violation of O.C.G.A. § 10-1-372(a), including:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or

grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

616. Marriott's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Georgia Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Georgia Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Georgia Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not

comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

617. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

618. Marriott intended to mislead Plaintiff and Georgia Subclass members and induce them to rely on its misrepresentations and omissions.

619. In the course of its business, Marriott engaged in activities with a tendency or capacity to deceive.

620. Marriott acted intentionally, knowingly, and maliciously to violate Georgia's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Georgia Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

621. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as Secure and was trusted with sensitive and valuable Personal Information regarding millions of consumers, including Plaintiff and the Georgia Subclass.

622. Marriott accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public.

623. Plaintiff and the Georgia Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

624. As a direct and proximate result of Marriott's deceptive trade practices, Plaintiff

and Georgia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

625. Plaintiff and Georgia Subclass members seek all relief allowed by law, including injunctive relief, and reasonable attorneys' fees and costs, under O.C.G.A. § 10-1-373.

CLAIMS ON BEHALF OF THE HAWAII SUBCLASS

COUNT 25

HAWAII SECURITY BREACH NOTIFICATION ACT,

Haw. Rev. Stat. §§ 487N-1, et seq.

626. Hawaii Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

627. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Haw. Rev. Stat. § 487N-2(a).

628. Plaintiff and Hawaii Subclass members' PII includes Personal Information as covered under Haw. Rev. Stat. § 487N-2(a).

629. Marriott is required to accurately notify Plaintiff and Hawaii Subclass members if it becomes aware of a breach of its data security system without unreasonable delay under Haw. Rev. Stat. § 487N-2(a).

630. Because Marriott was aware of a breach of its security system, it had an obligation to disclose the Marriott data breach in a timely and accurate fashion as mandated by Haw. Rev. Stat. § 487N-2(a).

631. By failing to disclose the Marriott data breach in a timely and accurate manner,

Marriott violated Haw. Rev. Stat. § 487N-2(a).

632. As a direct and proximate result of Marriott's violations of Haw. Rev. Stat. § 487N-2(a), Plaintiff and Hawaii Subclass members suffered damages, as described above.

633. Plaintiff and Hawaii Subclass members seek relief under Haw. Rev. Stat. § 487N-3(b), including actual damages.

COUNT 26

HAWAII UNFAIR PRACTICES AND UNFAIR COMPETITION ACT,

Haw. Rev. Stat. §§ 480-1, et seq.

634. Hawaii Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

635. Plaintiff and Hawaii Subclass members are "consumers" as defined by Haw. Rev. Stat. § 480-1.

636. Plaintiffs, the Hawaii Subclass members, and Defendants are "persons" as defined by Haw. Rev. Stat. § 480-1.

637. Marriott advertised, offered, or sold goods or services in Hawaii and engaged in trade or commerce directly or indirectly affecting the people of Hawaii.

638. Marriott engaged in unfair or deceptive acts or practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the goods and services purchased by Hawaii Subclass members in violation of Haw. Rev. Stat. § 480-2(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Hawaii Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate

identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Hawaii Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Hawaii Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

639. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

640. Marriott intended to mislead Plaintiff and Hawaii Subclass members and induce them to rely on its misrepresentations and omissions.

641. The foregoing unlawful and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous.

642. Marriott acted intentionally, knowingly, and maliciously to violate Hawaii's Unfair Practices and Unfair Competition Act, and recklessly disregarded Plaintiff and Hawaii Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

643. As a direct and proximate result of Marriott's deceptive acts and practices, Plaintiff and Hawaii Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

644. Plaintiff and Hawaii Subclass members seek all monetary and nonmonetary relief allowed by law, including actual damages, benefit of the bargain damages, treble damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT 27

HAWAII UNIFORM DECEPTIVE TRADE PRACTICE ACT,

Haw. Rev. Stat. §§ 481A-3, et seq.

645. Hawaii Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

646. Plaintiff and Hawaii Subclass members are "persons" as defined by Haw. Rev. Stat. § 481A-2.

647. Marriott engaged in unfair and deceptive trade practices in the conduct of its business, violating Haw. Rev. Stat. § 481A-3, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

648. Marriott's unfair and deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Hawaii Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Hawaii Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Hawaii Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not

comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

649. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

650. The above unfair and deceptive practices and acts by Marriott were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Hawaii Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

651. As a direct and proximate result of Marriott's unfair, unlawful, and deceptive trade practices, Plaintiff and Hawaii Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

652. Plaintiff and Hawaii Subclass members seek all monetary and nonmonetary relief allowed by law, including injunctive relief, attorneys' fees and costs, and any other relief that the Court deems proper

CLAIMS ON BEHALF OF THE ILLINOIS SUBCLASS

COUNT 28

ILLINOIS PERSONAL INFORMATION PROTECTION ACT

815 Ill. Comp. Stat. §§ 530/10(a), et seq.

653. Illinois Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeat and allege all previous Paragraphs, as if

fully alleged herein.

654. As a publicly held corporation which handles, collects, disseminates, and otherwise deals with nonpublic personal information, Marriott is a Data Collector as defined in 815 Ill. Comp. Stat. § 530/5.

655. Plaintiff and Illinois Subclass members' PII includes Personal Information as covered under 815 Ill. Comp. Stat. § 530/5.

656. As a Data Collector, Marriott is required to notify Plaintiffs and Illinois Subclass members of a breach of its data security system in the most expedient time possible and without unreasonable delay pursuant to 815 Ill. Comp. Stat. § 530/10(a).

657. By failing to disclose the Breach in the most expedient time possible and without unreasonable delay, Marriott violated 815 Ill. Comp. Stat. § 530/10(a).

658. Pursuant to 815 Ill. Comp. Stat. § 530/20, a violation of 815 Ill. Comp. Stat. § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

659. As a direct and proximate result of Marriott's violations of 815 Ill. Comp. Stat. § 530/10(a), Plaintiffs and Illinois Subclass members suffered damages, as described above.

660. Plaintiffs and Connecticut Subclass members seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered because of Marriott's willful violations of 815 Ill. Comp. Stat. § 530/10(a), including actual damages, equitable relief, costs, and attorneys' fees.

COUNT 29

ILLINOIS CONSUMER FRAUD ACT

815 Ill. Comp. Stat. §§ 505, et seq.

661. Illinois Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

662. Marriott is a “person” as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

663. Plaintiffs and Illinois Subclass members are “consumers” as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

664. Marriott’s conduct as described herein was in the conduct of “trade” or “commerce” as defined by 815 Ill. Comp. Stat. § 505/1(f).

665. Marriott’s deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Illinois Subclass members’ Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Illinois Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Illinois Subclass members’ Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Illinois Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, and the Illinois Uniform

Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Illinois Subclass members' Personal Information; and

g Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

666. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

667. Marriott intended to mislead Plaintiffs and Illinois Subclass members and induce them to rely on its misrepresentations and omissions.

668. The above unfair and deceptive practices and acts by Marriott were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

669. Marriott acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiffs and Illinois Subclass members' rights. Past breaches put Marriott on notice that its security and privacy protections were inadequate.

670. As a direct and proximate result of Marriott's unfair, unlawful, and deceptive acts and practices, Plaintiffs and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial

accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

671. Plaintiffs and Illinois Subclass members seek all monetary and nonmonetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT 30

ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT

815 Ill. Comp. Stat. §§ 510/2, et seq.

672. Illinois Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

673. Marriott is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

674. Marriott engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised; and
- d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

675. Marriott's deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Illinois Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Illinois Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Illinois Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

676. Marriott's representations and omissions were material because they were likely to

deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

677. The above unfair and deceptive practices and acts by Marriott were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Illinois Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

678. As a direct and proximate result of Marriott's unfair, unlawful, and deceptive trade practices, Plaintiffs and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

679. Plaintiff and Illinois Subclass members seek all monetary and nonmonetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

CLAIMS ON BEHALF OF THE INDIANA SUBCLASS

COUNT 31

INDIANA DECEPTIVE CONSUMER SALES ACT

Ind. Code §§ 24-5-0.5-1, et seq.

680. Indiana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Indiana Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

681. Marriott is a "person" as defined by Ind. Code § 24-5-0.5-2(a)(2).

682. Marriott is a "supplier" as defined by § 24-5-0.5-2(a)(1), because it regularly engages in or solicits "consumer transactions," within the meaning of § 24-5-0.5-2(a)(3)(A).

683. Marriott engaged in unfair, abusive, and deceptive acts, omissions, and practices in

connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3(a).

684. Marriott's representations and omissions include both implicit and explicit representations.

685. Marriott's unfair, abusive, and deceptive acts, omissions, and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Indiana Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Indiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c), which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Indiana Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Indiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Indiana Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not

comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Indiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c).

686. Marriott's acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

687. The injury to consumers from Marriott's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their Personal Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant number of consumers, but also because it inflicted a significant amount of harm on each consumer.

688. Consumers could not have reasonably avoided injury because Marriott's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Marriott created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

689. Marriott's inadequate data security had no countervailing benefit to consumers or to competition.

690. Marriott's acts and practices were "abusive" for numerous reasons, including:

a. Because they materially interfered with consumers' ability to understand a term or condition in a consumer transaction. Marriott's failure to disclose the inadequacies in its data security interfered with consumers' decision-making in a variety of their transactions.

b. Because they took unreasonable advantage of consumers' lack of understanding about the material risks, costs, or conditions of a consumer transaction. Without knowing about the inadequacies in Marriott's data security, consumers lacked an understanding of

the material risks and costs of a variety of their transactions.

c. Because they took unreasonable advantage of consumers' inability to protect their own interests. Consumers could not protect their interests due to the asymmetry in information between them and Marriott concerning the state of Marriott's security.

d. Because Marriott took unreasonable advantage of consumers' reasonable reliance that it was acting in their interests to secure their data. Consumers' reliance was reasonable.

691. Marriott also engaged in "deceptive" acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including:

a. Misrepresenting that the subject of a consumer transaction has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have;

b. Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not; and

c. Misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (i.e., more data security) than the supplier intends or reasonably expects.

692. Marriott intended to mislead Plaintiff and Indiana Subclass members and induce them to rely on its misrepresentations and omissions.

693. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

694. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business

and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as secure and was trusted with sensitive and valuable Personal Information regarding millions of consumers, including Plaintiff and the Indiana Subclass.

695. Marriott accepted the responsibility of being a “steward of data” while keeping the inadequate state of its security controls secret from the public.

696. Plaintiff and the Indiana Subclass members acted reasonably in relying on Marriott’s misrepresentations and omissions, the truth of which they could not have discovered.

697. Marriott had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensiveness of the Personal Information in its possession, and the generally accepted professional standards in the industry. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Indiana Subclass—and Marriott, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott. Marriott’s duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and prior data breaches, while purposefully withholding material facts from Plaintiff and the Indiana Subclass that contradicted these representations.

698. Marriott acted intentionally, knowingly, and maliciously to violate Indiana’s Deceptive Consumer Sales Act, and recklessly disregarded Plaintiff and Indiana Subclass members’ rights. Past breaches put it on notice that its security and privacy protections were inadequate. Marriott’s actions were not the result of a mistake of fact or law, honest error or judgment, overzealousness, mere negligence, or other human failing.

699. Plaintiff sent a demand for relief on behalf of the Indiana Subclass pursuant to Ind. Code § 24-5-0.5-5 on December 11, 2018. Marriott has not cured its unfair, abusive, and deceptive acts and practices, or its violations of Indiana Deceptive Consumer Sales Act were incurable.

700. Since Plaintiff provided the requisite notice, Marriott has failed to cure its violations of the Indiana Deceptive Consumer Sales Act.

701. Marriott's conduct includes incurable deceptive acts that Marriott engaged in as part of a scheme, artifice, or device with intent to defraud or mislead, under Ind. Code § 24-5-0.5-2(a)(8).

702. As a direct and proximate result of Marriott's uncured or incurable unfair, abusive, and deceptive acts or practices, Plaintiff and Indiana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

703. Marriott's violations present a continuing risk to Plaintiff and Indiana Subclass members as well as to the general public.

704. Plaintiff and Indiana Subclass members seek all monetary and nonmonetary relief allowed by law, including the greater of actual damages or \$500 for each non-willful violation; the greater of treble damages or \$1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

CLAIMS ON BEHALF OF THE IOWA SUBCLASS

COUNT 32

PERSONAL INFORMATION SECURITY BREACH PROTECTION LAW,

Iowa Code § 715C.2

705. Iowa Plaintiff(s) identified above ("Plaintiff," for purposes of this Count),

individually and on behalf of the Iowa Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

706. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Iowa Code § 715C.2(1).

707. Plaintiff's and Iowa Subclass members' PII includes Personal Information as covered under Iowa Code § 715C.2(1).

708. Marriott is required to accurately notify Plaintiff and Iowa Subclass members if it becomes aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Iowa Code § 715C.2(1).

709. Because Marriott was aware of a breach of its security system, Marriott had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Iowa Code § 715C.2(1).

710. By failing to disclose the Marriott data breach in a timely and accurate manner, Marriott violated Iowa Code § 715C.2(1).

711. Pursuant to Iowa Code § 715C.2(9), a violation of Iowa Code § 715C.2(1) is an unlawful practice pursuant to Iowa Code Ann. § 714.16(7).

712. As a direct and proximate result of Marriott's violations of Iowa Code § 715C.2(1), Plaintiff and Iowa Subclass members suffered damages, as described above.

713. Plaintiff and Iowa Subclass members seek relief under Iowa Code § 714.16(7), including actual damages and injunctive relief.

COUNT 33

IOWA PRIVATE RIGHT OF ACTION FOR CONSUMER FRAUDS ACT,

Iowa Code § 714H

714. Iowa Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Iowa Subclass, repeats and alleges all previous Paragraphs, as if

fully alleged herein.

715. Marriott is a “person” as defined by Iowa Code § 714H.2(7).

716. Plaintiff and Iowa Subclass members are “consumers” as defined by Iowa Code § 714H.2(3).

717. Marriott’s conduct described herein related to the “sale” or “advertisement” of “merchandise” as defined by Iowa Code §§ 714H.2(2), (6), & (8).

718. Marriott engaged in unfair, deceptive, and unconscionable trade practices, in violation of the Iowa Private Right of Action for Consumer Frauds Act, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Iowa Subclass members’ Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Iowa Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Iowa Subclass members’ Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Iowa Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not

reasonably or adequately secure Plaintiff and Iowa Subclass members' Personal Information; and

g Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Iowa Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

719. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

720. Marriott intended to mislead Plaintiff and Iowa Subclass members and induce them to rely on its misrepresentations and omissions.

721. Marriott acted intentionally, knowingly, and maliciously to violate Iowa's Private Right of Action for Consumer Frauds Act, and recklessly disregarded Plaintiff and Iowa Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

722. As a direct and proximate result of Marriott's unfair, deceptive, and unconscionable conduct, Plaintiff and Iowa Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

723. Plaintiff and Iowa Subclass members seek all monetary and nonmonetary relief allowed by law, including injunctive relief, damages, punitive damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE KANSAS SUBCLASS

COUNT 34

PROTECTION OF CONSUMER INFORMATION

Kan. Stat. Ann. §§ 50-7a02(a), et seq.

724. Kansas Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Kansas Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

725. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Kan. Stat. Ann. § 50-7a02(a).

726. Plaintiff’s and Kansas Subclass members’ PII includes Personal Information as covered under Kan. Stat. Ann. § 50-7a02(a).

727. Marriott is required to accurately notify Plaintiff and Kansas Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have caused misuse of Plaintiff’s and Kansas Subclass members’ Personal Information, in the most expedient time possible and without unreasonable delay under Kan. Stat. Ann. § 50-7a02(a).

728. Because Marriott was aware of a breach of its security system that was reasonably likely to have caused misuse of Plaintiffs’ and Kansas Subclass members’ Personal Information, Marriott had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Kan. Stat. Ann. § 50-7a02(a).

729. By failing to disclose the Breach in a timely and accurate manner, Marriott violated Kan. Stat. Ann. § 50-7a02(a).

730. As a direct and proximate result of Marriott’s violations of Kan. Stat. Ann. § 50-7a02(a), Plaintiff and Kansas Subclass members suffered damages, as described above.

731. Plaintiff and Kansas Subclass members seek relief under Kan. Stat. Ann. § 50-7a02(g), including equitable relief.

COUNT 35

KANSAS CONSUMER PROTECTION ACT

K.S.A. §§ 50-623, et seq.

732. Kansas Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Kansas Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

733. 730. K.S.A. §§ 50-623, et seq. is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

734. Plaintiff and Kansas Subclass members are “consumers” as defined by K.S.A. § 50-624(b).

735. The acts and practices described herein are “consumer transactions,” as defined by K.S.A. § 50-624(c).

736. Marriott is a “supplier” as defined by K.S.A. § 50-624(l).

737. Marriott advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

738. Marriott engaged in deceptive and unfair acts or practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Kansas Subclass members’ Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Kansas’s identity fraud statute, the Wayne

Owen Act, K.S.A. § 50-6,139b, which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Kansas Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Kansas Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b.

739. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

740. Marriott intended to mislead Plaintiff and Kansas Subclass members and induce them to rely on its misrepresentations and omissions.

741. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as secure and was trusted with sensitive and valuable Personal Information regarding millions of consumers, including Plaintiff and the Kansas Subclass.

742. Marriott accepted the responsibility of being a “steward of data” while keeping the inadequate state of its security controls secret from the public.

743. Plaintiff and the Kansas Subclass members acted reasonably in relying on Marriott’s misrepresentations and omissions, the truth of which they could not have discovered.

744. Marriott also engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of K.S.A. § 50-627, including:

a. Knowingly taking advantage of the inability of Plaintiff and the Kansas Subclass to reasonably protect their interests, due to their lack of knowledge (see K.S.A. § 50-627(b)(1)); and

b. Requiring Plaintiff and the Kansas Subclass to enter into a consumer transaction on terms that Marriott knew were substantially one-sided in favor of Marriott (see K.S.A. § 50-627(b)(5)).

745. Plaintiff and the Kansas Subclass had unequal bargaining power with respect to their ability to control the security and confidentiality of their Personal Information in Marriott’s possession.

746. The above unfair, deceptive, and unconscionable practices and acts by Marriott were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kansas Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

747. Marriott acted intentionally, knowingly, and maliciously to violate Kansas’s Consumer Protection Act, and recklessly disregarded Plaintiff and Kansas Subclass members’ rights. Past breaches put it on notice that its security and privacy protections were inadequate.

748. As a direct and proximate result of Marriott’s unfair, deceptive, and unconscionable trade practices, Plaintiff and Kansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages,

including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

749. Plaintiff and Kansas Subclass members seek all monetary and nonmonetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under K.S.A. §§ 50-634 and 50-636; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE KENTUCKY SUBCLASS

COUNT 36

KENTUCKY COMPUTER SECURITY BREACH NOTIFICATION ACT

Ky. Rev. Stat. Ann. §§ 365.732, et seq.

750. Kentucky Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Kentucky Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

751. Marriott is required to accurately notify Plaintiffs and Kentucky Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiffs' and Kentucky Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under Ky. Rev. Stat. Ann. § 365.732(2).

752. Marriott is a business that holds computerized data that includes Personal Information as defined by Ky. Rev. Stat. Ann. § 365.732(2).

753. Plaintiffs' and Kentucky Subclass members' PII includes Personal Information as covered under Ky. Rev. Stat. Ann. § 365.732(2).

754. Because Marriott was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiffs' and Kentucky Subclass members' Personal Information, Marriott had an obligation to disclose the data breach in a timely and

accurate fashion as mandated by Ky. Rev. Stat. Ann. § 365.732(2).

755. By failing to disclose the Breach in a timely and accurate manner, Marriott violated Ky. Rev. Stat. Ann. § 365.732(2).

756. As a direct and proximate result of Marriott's violations of Ky. Rev. Stat. Ann. § 365.732(2), Plaintiffs and Kentucky Subclass members suffered damages, as described above.

757. Plaintiff and Kentucky Subclass members seek relief under Ky. Rev. Stat. Ann. § 446.070, including actual damages.

COUNT 37

KENTUCKY CONSUMER PROTECTION ACT

Ky. Rev. Stat. §§ 367.110, et seq.

758. Kentucky Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Kentucky Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

759. Marriott is a "person" as defined by Ky. Rev. Stat. § 367.110(1).

760. Marriott advertised, offered, or sold goods or services in Kentucky and engaged in trade or commerce directly or indirectly affecting the people of Kentucky, as defined by Ky. Rev. Stat. 367.110(2).

761. Marriott engaged in unfair, false, misleading, deceptive, and unconscionable acts or practices, in violation of Ky. Rev. Stat. § 367.170, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Kentucky Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kentucky Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Kentucky Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Kentucky Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Kentucky Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kentucky Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

762. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

763. Marriott intended to mislead Plaintiffs and Kentucky Subclass members and induce them to rely on its misrepresentations and omissions.

764. Plaintiffs and Kentucky Subclass members' purchased goods or services for personal, family, or household purposes and suffered ascertainable losses of money or property as a result of Marriott's unlawful acts and practices.

765. The above unlawful acts and practices by Marriott were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Kentucky Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

766. Marriott acted intentionally, knowingly, and maliciously to violate Kentucky's Consumer Protection Act, and recklessly disregarded Plaintiffs and Kentucky Subclass members' rights. Past breaches put it on notice that its security and privacy protections were inadequate.

767. As a direct and proximate result of Marriott's unlawful acts and practices, Plaintiffs and Kentucky Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

768. Plaintiffs and Kentucky Subclass members seek all monetary and nonmonetary relief allowed by law, including damages, punitive damages, restitution or other equitable relief, injunctive relief, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE LOUISIANA SUBCLASS

COUNT 38

DATABASE SECURITY BREACH NOTIFICATION LAW,

La. Rev. Stat. Ann. §§ 51:3074(A), et seq.

769. Louisiana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

770. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by La. Rev. Stat. Ann. § 51:3074(C).

771. Plaintiff's and Louisiana Subclass members' PII includes Personal Information as covered under La. Rev. Stat. Ann. § 51:3074(C).

772. Marriott is required to accurately notify Plaintiff and Louisiana Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under La. Rev. Stat. Ann. § 51:3074(C).

773. Because Marriott was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass members' Personal Information, Marriott had an obligation to disclose the Marriott data breach in a timely and accurate fashion as mandated by La. Rev. Stat. Ann. § 51:3074(C).

774. By failing to disclose the Marriott data breach in a timely and accurate manner, Marriott violated La. Rev. Stat. Ann. § 51:3074(C).

775. As a direct and proximate result of Marriott's violations of La. Rev. Stat. Ann. § 51:3074(C), Plaintiff and Louisiana Subclass members suffered damages, as described above.

776. Plaintiff and Louisiana Subclass members seek relief under La. Rev. Stat. Ann. § 51:3075, including actual damages.

COUNT 39

LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW,

La. Rev. Stat. Ann. §§ 51:1401, et seq.

777. Louisiana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

778. Marriott, Plaintiff, and the Louisiana Subclass members are "persons" within the meaning of the La. Rev. Stat. Ann. § 51:1402(8).

779. Plaintiff and Louisiana Subclass members are “consumers” within the meaning of La. Rev. Stat. Ann. § 51:1402(1).

780. Marriott engaged in “trade” or “commerce” within the meaning of La. Rev. Stat. Ann. § 51:1402(10).

781. The Louisiana Unfair Trade Practices and Consumer Protection Law (“Louisiana CPL”) makes unlawful “unfair or deceptive acts or practices in the conduct of any trade or commerce.” La. Rev. Stat. Ann. § 51:1405(A). Unfair acts are those that offend established public policy, while deceptive acts are practices that amount to fraud, deceit, or misrepresentation.

782. Marriott participated in unfair and deceptive acts and practices that violated the Louisiana CPL, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Louisiana Subclass members’ Personal Information, which was a direct and proximate cause of the Breach;

- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Breach;

- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Louisiana Subclass members’ Personal Information, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members’ Personal

Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Louisiana Subclass members' Personal Information; and

g Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

783. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

784. Marriott intended to mislead Plaintiff and Louisiana Subclass members and induce them to rely on its misrepresentations and omissions.

785. Marriott's unfair and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

786. Marriott acted intentionally, knowingly, and maliciously to violate Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Louisiana Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

787. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as secure and was trusted with sensitive and valuable Personal

Information regarding hundreds of millions of consumers, including Plaintiff and the Louisiana Subclass.

788. Marriott accepted the responsibility of being a “steward of data” while keeping the inadequate state of its security controls secret from the public.

789. Plaintiff and the Louisiana Subclass members acted reasonably in relying on Marriott’s misrepresentations and omissions, the truth of which they could not have discovered.

790. As a direct and proximate result of Marriott’s unfair and deceptive acts and practices, Plaintiff and Louisiana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

Plaintiff and Louisiana Subclass members seek all monetary and nonmonetary relief allowed by law, including actual damages; treble damages for Marriott’s knowing violations of the Louisiana CPL; declaratory relief; attorneys’ fees; and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE MARYLAND SUBCLASS

COUNT 40

MARYLAND PERSONAL INFORMATION PROTECTION ACT

Md. Comm. Code §§ 14-3501, et seq.

791. Maryland Plaintiffs identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the Maryland Subclass, repeat and alleges all previous Paragraphs, as if fully alleged herein.

792. Under Md. Comm. Code § 14-3503(a), “[t]o protect Personal Information from unauthorized access, use, modification, or disclosure, a business that owns or licenses Personal Information of an individual residing in the State shall implement and maintain reasonable security

procedures and practices that are appropriate to the nature of Personal Information owned or licensed and the nature and size of the business and its operations.”

793. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Md. Comm. Code §§ 14-3501(b)(1) and (2).

794. Plaintiffs and Maryland Subclass members are “individuals” and “customers” as defined and covered by Md. Comm. Code §§ 14-3502(a) and 14- 3503.

795. Plaintiffs’ and Maryland Subclass members’ PII includes Personal Information as covered under Md. Comm. Code § 14-3501(d).

796. Marriott did not maintain reasonable security procedures and practices appropriate to the nature of the Personal Information owned or licensed and the nature and size of its business and operations in violation of Md. Comm. Code § 14-3503.

797. The Breach was a “breach of the security of a system” as defined by Md. Comm. Code § 14-3504(1).

798. Under Md. Comm. Code § 14-3504(b)(1), “[a] business that owns or licenses computerized data that includes Personal Information of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that Personal Information of the individual has been or will be misused as a result of the breach.”

799. Under Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), “[i]f, after the investigation is concluded, the business determines that misuse of the individual’s Personal Information has occurred or is reasonably likely to occur as a result of a breach of the security system, the business shall notify the individual of the breach” and that notification “shall be given as soon as reasonably practical after the business discovers or is notified of the breach of a security system.”

800. Because Marriott discovered a security breach and had notice of a security breach,

Marriott had an obligation to disclose the Breach in a timely and accurate fashion as mandated by Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

801. By failing to disclose the Breach in a timely and accurate manner, Marriott violated Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

802. As a direct and proximate result of Marriott's violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), Plaintiffs and Maryland Subclass members suffered damages, as described above. 818. Pursuant to Md. Comm. Code § 14-3508, Marriott's violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of the Maryland Consumer Protection Act, 13 Md. Comm. Code §§ 13-101, et seq. and subject to the enforcement and penalty provisions contained within the Maryland Consumer Protection Act.

803. Plaintiffs and Maryland Subclass members seek relief under Md. Comm. Code § 13-408, including actual damages and attorney's fees.

COUNT 41

MARYLAND CONSUMER PROTECTION ACT

Md. Comm. Code §§ 13-301, et seq.

804. Maryland Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Maryland Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

805. Marriott is a person as defined by Md. Comm. Code § 13-101(h).

806. Marriott's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by Md. Comm. Code § 13-101(i) and § 13-303.

807. Maryland Subclass members are "consumers" as defined by Md. Comm. Code § 13-101(c).

808. Marriott advertises, offers, or sell "consumer goods" or "consumer services" as

defined by Md. Comm. Code § 13-101(d).

809. Marriott advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland.

810. Marriott engaged in unfair and deceptive trade practices, in violation of Md. Comm. Code § 13-301, including:

- a. False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;
- b. Representing that consumer goods or services have a characteristic that they do not have;
- c. Representing that consumer goods or services are of a particular standard, quality, or grade that they are not;
- d. Failing to state a material fact where the failure deceives or tends to deceive;
- e. Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered;
- f. Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale lease or rental.

811. Marriott engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services or with respect to the extension of consumer credit, in violation of Md. Comm. Code § 13- 303, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Maryland Subclass members' Personal Information, which was a direct and proximate cause of the Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate

identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Maryland Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503, which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Maryland Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Maryland Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Maryland Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Maryland Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503.

812. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information. Marriott's misrepresentations and

omissions would have been important to a significant number of consumers in making financial decisions.

813. Marriott intended to mislead Plaintiffs and Maryland Subclass members and induce them to rely on its misrepresentations and omissions.

814. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as secure and was trusted with sensitive and valuable Personal Information regarding millions of consumers, including Plaintiff and the Maryland Subclass.

815. Marriott accepted the responsibility of being a “steward of data” while keeping the inadequate state of its security controls secret from the public.

816. Plaintiffs and the Maryland Subclass members acted reasonably in relying on Marriott’s misrepresentations and omissions, the truth of which they could not have discovered.

817. Marriott acted intentionally, knowingly, and maliciously to violate Maryland’s Consumer Protection Act, and recklessly disregarded Plaintiffs and Maryland Subclass members’ rights. Past breaches put it on notice that its security and privacy protections were inadequate.

818. As a direct and proximate result of Marriott’s unfair and deceptive acts and practices, Plaintiffs and Maryland Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

819. Plaintiffs and Maryland Subclass members seek all monetary and nonmonetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys’ fees and costs.

CLAIMS ON BEHALF OF THE MASSACHUSETTS SUBCLASS

COUNT 42

MASSACHUSETTS CONSUMER PROTECTION ACT

Mass. Gen. Laws Ann. Ch. 93A, §§ 1, et seq.

820. Massachusetts Plaintiffs identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the Massachusetts Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

821. Marriott and Massachusetts Subclass members are “persons” as meant by Mass. Gen. Laws Ann. Ch. 93A, § 1(a).

822. Marriott operates in “trade or commerce” as meant by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

823. Marriott advertised, offered, or sold goods or services in Massachusetts and engaged in trade or commerce directly or indirectly affecting the people of Massachusetts, as defined by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

824. Plaintiffs sent a demand for relief on behalf of the Massachusetts Subclass pursuant to Mass. Gen. Laws Ann. Ch. 93A § 9(3) on December 11, 2018.

825. Marriott engaged in unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws Ann. Ch. 93A, § 2(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Massachusetts Subclass members’ Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Massachusetts Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05, which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Massachusetts Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Massachusetts Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Massachusetts Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Massachusetts Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05.

826. Marriott's acts and practices were "unfair" because they fall within the penumbra of common law, statutory, and established concepts of unfairness, given that Marriott solely held the true facts about its inadequate security for Personal Information, which Plaintiffs and the Massachusetts Subclass members could not independently discover.

827. Consumers could not have reasonably avoided injury because Marriott's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Marriott created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

828. Marriott's inadequate data security had no countervailing benefit to consumers or to competition.

829. Marriott intended to mislead Plaintiffs and Massachusetts Subclass members and induce them to rely on its misrepresentations and omissions.

830. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

831. Marriott acted intentionally, knowingly, and maliciously to violate Massachusetts's Consumer Protection Act, and recklessly disregarded Plaintiffs and Massachusetts Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

832. As a direct and proximate result of Marriott's unfair and deceptive, Plaintiffs and Massachusetts Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

833. Plaintiffs and Massachusetts Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, double or treble damages, injunctive or other equitable relief, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE MICHIGAN SUBCLASS

COUNT 43

MICHIGAN IDENTITY THEFT PROTECTION ACT

Mich. Comp. Laws Ann. §§ 445.72, et seq.

834. Michigan Plaintiffs identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the Michigan Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

835. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Mich. Comp. Laws Ann. § 445.72(1).

836. Plaintiffs’ and Michigan Subclass members’ PII includes Personal Information as covered under Mich. Comp. Laws Ann. § 445.72(1).

837. Marriott is required to accurately notify Plaintiffs and Michigan Subclass members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

838. Because Marriott discovered a security breach and had notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), Marriott had an obligation to disclose the Breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

839. By failing to disclose the Breach in a timely and accurate manner, Marriott violated Mich. Comp. Laws Ann. § 445.72(4).

840. As a direct and proximate result of Marriott’s violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiffs and Michigan Subclass members suffered damages, as described above.

841. Plaintiffs and Michigan Subclass members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including a civil fine.

COUNT 44

MICHIGAN CONSUMER PROTECTION ACT

Mich. Comp. Laws Ann. §§ 445.903, et seq.

842. Michigan Plaintiffs identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the Michigan Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

843. Marriott and Michigan Subclass members are “persons” as defined by Mich. Comp. Laws Ann. § 445.903(d).

844. Marriott advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

845. Marriott engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c);

b. Representing that its goods and services are of a particular standard or quality if they are of another in violation of Mich. Comp. Laws Ann. § 445.903(1)(e);

c. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb); and

d. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).

846. Marriott’s unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures

to protect Plaintiff and Michigan Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Michigan Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Michigan Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Michigan Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Michigan Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Michigan Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

847. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

848. Marriott intended to mislead Plaintiffs and Michigan Subclass members and induce them to rely on its misrepresentations and omissions.

849. Marriott acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiffs and Michigan Subclass members' rights. Past breaches put it on notice that its security and privacy protections were inadequate.

850. As a direct and proximate result of Marriott's unfair, unconscionable, and deceptive practices, Plaintiffs and Michigan Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

851. Plaintiffs and Michigan Subclass members seek all monetary and nonmonetary relief allowed by law, including the greater of actual damages or \$250, injunctive relief, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE MINNESOTA SUBCLASS

COUNT 45

MINNESOTA CONSUMER FRAUD ACT,

Minn. Stat. §§ 325F.68, et seq. and Minn. Stat. §§ 8.31, et seq.

852. Minnesota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Minnesota Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

853. Marriott, Plaintiff, and members of the Minnesota Subclass are each a "person" as defined by Minn. Stat. § 325F.68(3).

854. Marriott's goods, services, commodities, and intangibles are "merchandise" as defined by Minn. Stat. § 325F.68(2).

855. Marriott engaged in “sales” as defined by Minn. Stat. § 325F.68(4).

856. Marriott engaged in fraud, false pretense, false promise, misrepresentation, misleading statements, and deceptive practices in connection with the sale of merchandise, in violation of Minn. Stat. § 325F.69(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Minnesota Subclass members’ Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Minnesota Subclass members’ Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Minnesota Subclass members’ Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff

and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

857. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

858. Marriott intended to mislead Plaintiff and Minnesota Subclass members and induce them to rely on its misrepresentations and omissions.

859. Marriott's fraudulent, misleading, and deceptive practices affected the public interest, including millions of Minnesotans affected by the Breach.

860. As a direct and proximate result of Marriott's fraudulent, misleading, and deceptive practices, Plaintiff and Minnesota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

861. Plaintiff and Minnesota Subclass members seek all monetary and nonmonetary relief allowed by law, including damages; injunctive or other equitable relief; and attorneys' fees, disbursements, and costs.

COUNT 46

MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT,

Minn. Stat. §§ 325D.43, et seq.

862. Minnesota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Minnesota Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

863. By engaging in deceptive trade practices in the course of its business and vocation,

directly or indirectly affecting the people of Minnesota, Marriott violated Minn. Stat. § 325D.44, including the following provisions:

- a. Representing that its goods and services had characteristics, uses, and benefits that they did not have, in violation of Minn. Stat. § 325D.44(1)(5);
- b. Representing that goods and services are of a particular standard or quality when they are of another, in violation of Minn. Stat. § 325D.44(1)(7);
- c. Advertising goods and services with intent not to sell them as advertised, in violation of Minn. Stat. § 325D.44(1)(9); and
- d. Engaging in other conduct which similarly creates a likelihood of confusion or misunderstanding, in violation of Minn. Stat. § 325D.44(1)(13).

864. Marriott's deceptive practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Minnesota Subclass members' Personal Information, which was a direct and proximate cause of the Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Minnesota Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties

pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Minnesota Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

865. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

866. Marriott intended to mislead Plaintiff and Minnesota Subclass members and induce them to rely on its misrepresentations and omissions.

867. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as secure and was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Minnesota Subclass.

868. Marriott accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public.

869. Plaintiff and the Minnesota Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

870. Marriott acted intentionally, knowingly, and maliciously to violate Minnesota's

Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Minnesota Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

871. As a direct and proximate result of Marriott's deceptive trade practices, Plaintiff and Minnesota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information

872. Plaintiff and Minnesota Subclass members seek all monetary and nonmonetary relief allowed by law, including injunctive relief and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE MISSISSIPPI SUBCLASS

COUNT 47

MISSISSIPPI CONSUMER PROTECTION ACT,

Miss. Code §§ 75-24-1, et seq.

873. Mississippi Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Mississippi Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

874. Marriott is a "person," as defined by Miss. Code § 75-24-3.

875. Marriott advertised, offered, or sold goods or services in Mississippi and engaged in trade or commerce directly or indirectly affecting the people of Mississippi, as defined by Miss. Code § 75-24-3.

876. Marriott engaged in unfair and deceptive trade acts or practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Mississippi Subclass members' Personal Information, which was a direct

and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Mississippi Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Mississippi Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Mississippi Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Mississippi Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Mississippi Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

877. The above-described conduct violated Miss. Code Ann. § 75-24-5(2), including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;

b. Representing that goods or services are of a particular standard, quality, or

grade, or that goods are of a particular style or model, if they are of another; and

c. Advertising goods or services with intent not to sell them as advertised.

878. Marriott intended to mislead Plaintiffs and Mississippi Subclass members and induce them to rely on its misrepresentations and omissions.

879. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

880. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as secure and was trusted with sensitive and valuable Personal Information regarding millions of consumers, including Plaintiffs and the Mississippi Subclass.

881. Marriott accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public.

882. Plaintiff and the Mississippi Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

883. Marriott had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the Personal Information in its possession, and the generally accepted professional standards. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiffs and the Mississippi Subclass—and Marriott, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott.

884. Marriott's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and the Mississippi Subclass that contradicted these representations.

885. Marriott acted intentionally, knowingly, and maliciously to violate Mississippi's Consumer Protection Act, and recklessly disregarded Plaintiffs and Mississippi Subclass members' rights. Past breaches put it on notice that its security and privacy protections were inadequate.

886. As a direct and proximate result of Marriott's unfair and deceptive acts or practices and Plaintiffs and Mississippi Subclass members' purchase of goods or services primarily for personal, family, or household purposes, Plaintiffs and Mississippi Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

887. Marriott's violations present a continuing risk to Plaintiffs and Mississippi Subclass members as well as to the general public.

888. Plaintiffs and Mississippi Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution and other relief under Miss. Code § 75-24-11, injunctive relief, punitive damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE MISSOURI SUBCLASS

COUNT 48

MISSOURI MERCHANDISE PRACTICES ACT,

Mo. Rev. Stat. §§ 407.010, et seq.

889. Missouri Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Missouri Subclass, repeats and alleges all previous Paragraphs, as

if fully alleged herein.

890. Marriott is a “person” as defined by Mo. Rev. Stat. § 407.010(5).

891. Marriott advertised, offered, or sold goods or services in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as defined by Mo. Rev. Stat. § 407.010(4), (6) and (7).

892. Plaintiff and Missouri Subclass members purchased or leased goods or services primarily for personal, family, or household purposes.

893. Marriott engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Rev. Stat. § 407.020(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Missouri Subclass members’ Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Marriott data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Missouri Subclass members’ Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass members’ Personal

Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Missouri Subclass members' Personal Information; and

g Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

894. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

895. Marriott intended to mislead Plaintiff and Missouri Subclass members and induce them to rely on its misrepresentations and omissions.

896. Marriott acted intentionally, knowingly, and maliciously to violate Missouri's Merchandise Practices Act, and recklessly disregarded Plaintiff and Missouri Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

897. As a direct and proximate result of Marriott's unlawful, unfair, and deceptive acts and practices, Plaintiff and Missouri Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

898. Plaintiff and Missouri Subclass members seek all monetary and nonmonetary relief allowed by law, including actual damages, punitive damages, attorneys' fees and costs, injunctive

relief, and any other appropriate relief.

CLAIMS ON BEHALF OF THE MONTANA SUBCLASS

COUNT 49

COMPUTER SECURITY BREACH LAW,

Mont. Code Ann. §§ 30-14-1704(1), et seq.

899. Montana Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Montana Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

900. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Mont. Code Ann. § 30-14-1704(4)(b).

901. Marriott also maintains computerized data that includes Personal Information which Marriott does not own. Accordingly, it is subject to Mont. Code Ann. § 30-14-1704(1) and (2).

902. Plaintiff’s and Montana Subclass members’ PII includes Personal Information covered by Mont. Code Ann. § 30-14-1704(4)(b).

903. Marriott is required to give immediate notice of a breach of security of a data system to owners of Personal Information which Marriott does not own, including Plaintiff and Montana Subclass members, pursuant to Mont. Code Ann. § 30-14-1704(2).

904. Marriott is required to accurately notify Plaintiff and Montana Subclass members if it discovers a security breach, or receives notice of a security breach which may have compromised Personal Information which Marriott owns or licenses, without unreasonable delay under Mont. Code Ann. § 30-14-1704(1).

905. Because Marriott was aware of a security breach, Marriott had an obligation to disclose the data breach as mandated by Mont. Code Ann. § 30-14-1704(1) and (2).

906. Pursuant to Mont. Code Ann. § 30-14-1705, violations of Mont. Code Ann. § 30-14-1704 are unlawful practices under Mont. Code Ann. § 30-14-103, Montana’s Consumer

Protection Act.

907. As a direct and proximate result of Marriott's violations of Mont. Code Ann. § 30-14-1704(1) and (2), Plaintiff and Montana Subclass members suffered damages, as described above.

908. Plaintiff and Montana Subclass members seek relief under Mont. Code Ann. § 30-14-133, including actual damages and injunctive relief.

COUNT 50

MONTANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ACT,

M.C.A. §§ 30-14-101, et seq.

909. Montana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Montana Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

910. Marriott is a "person" as defined by MCA § 30-14-102(6).

911. Plaintiff and Montana Subclass members are "consumers" as defined by MCA § 30-14-102(1).

912. Marriott advertised, offered, or sold goods or services in Montana and engaged in trade or commerce directly or indirectly affecting the people of Montana, as defined by MCA § 30-14-102(8).

913. Marriott engaged in unfair and deceptive acts and practices in the conduct of trade or commerce, in violation MCA § 30-14-103, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Montana Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures

following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Montana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Marriott data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Montana Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Montana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Montana Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Montana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

914. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

915. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as secure and was trusted with sensitive and valuable Personal

Information regarding millions of consumers, including Plaintiff and the Montana Subclass.

916. Marriott accepted the responsibility of being a “steward of data” while keeping the inadequate state of its security controls secret from the public.

917. Plaintiff and the Montana Subclass members acted reasonably in relying on Marriott’s misrepresentations and omissions, the truth of which they could not have discovered.

918. Marriott’s acts described above are unfair and offend public policy; they are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers.

919. Marriott acted intentionally, knowingly, and maliciously to violate Montana’s Unfair Trade Practices and Consumer Protection Act, and recklessly disregarded Plaintiff and Montana Subclass members’ rights. Marriott’s numerous past data breaches put it on notice that its security and privacy protections were inadequate.

920. As a direct and proximate result of Marriott’s unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, Plaintiff and Montana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

921. Plaintiff and Montana Subclass members seek all monetary and nonmonetary relief allowed by law, including the greater of (a) actual damages or (b) statutory damages of \$500, treble damages, restitution, attorneys’ fees and costs, injunctive relief, and other relief that the Court deems appropriate.

CLAIMS ON BEHALF OF THE NEBRASKA SUBCLASS

COUNT 51

NEBRASKA CONSUMER PROTECTION ACT

Neb. Rev. Stat. §§ 59-1601, et seq.

922. Nebraska Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Nebraska Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

923. Marriott and Nebraska Subclass members are each a “person” as defined by Neb. Rev. Stat. § 59-1601(1).

924. Marriott advertised, offered, or sold goods or services in Nebraska and engaged in trade or commerce directly or indirectly affecting the people of Nebraska, as defined by Neb. Rev. Stat. § 59-1601.

925. Marriott engaged in unfair and deceptive acts and practices in conducting trade and commerce, in violation of Neb. Rev. Stat. § 59-1602, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Nebraska Subclass members’ Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of

Plaintiff and Nebraska Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Nebraska Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

926. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

927. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiffs and Nebraska Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

928. Marriott's unfair and deceptive acts and practices complained of herein affected the public interest, including the large percentage of Nebraskans affected by the Breach.

929. Plaintiff and Nebraska Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, the greater of either (1) actual damages or (2)

\$1,000, civil penalties, and reasonable attorneys' fees and costs.

COUNT 52

NEBRASKA UNIFORM DECEPTIVE TRADE PRACTICES ACT

Neb. Rev. Stat. §§ 87-301, et seq.

930. Nebraska Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Nebraska Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

931. Marriott and Nebraska Subclass members are "persons" as defined by Neb. Rev. Stat. § 87-301(19).

932. Marriott advertised, offered, or sold goods or services in Nebraska and engaged in trade or commerce directly or indirectly affecting the people of Nebraska.

933. Marriott engaged in deceptive trade practices in the course of its business, in violation of Neb. Rev. Stat. §§ 87-302(a)(5), (8), and (10), including:

a. Represented that goods and services have characteristics, uses, benefits, or qualities that they do not have;

b. Represented that goods and services are of a particular standard, quality, or grade if they are of another; and

c. Advertised its goods and services with intent not to sell them as advertised and in a manner calculated or tending to mislead or deceive.

934. Marriott's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Nebraska Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures

following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Nebraska Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Nebraska Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

935. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

936. Marriott intended to mislead Plaintiff and Nebraska Subclass members and induce them to rely on its misrepresentations and omissions.

937. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business

and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as secure and was trusted with sensitive and valuable Personal Information regarding millions of consumers, including Plaintiff and the Nebraska Subclass.

938. Marriott accepted the responsibility of being a “steward of data” while keeping the inadequate state of its security controls secret from the public.

939. Plaintiff and the Nebraska Subclass members acted reasonably in relying on Marriott’s misrepresentations and omissions, the truth of which they could not have discovered.

940. Marriott acted intentionally, knowingly, and maliciously to violate Nebraska’s Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Nebraska Subclass members’ rights. Past data breaches put it on notice that its security and privacy protections were inadequate.

941. As a direct and proximate result of Marriott’s deceptive trade practices, Plaintiff and Nebraska Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

942. Marriott’s deceptive trade practices complained of herein affected consumers at large, including the large percentage of Nebraskans affected by the Breach.

943. Plaintiff and Nebraska Subclass members seek all monetary and nonmonetary relief allowed by law, including injunctive relief, other equitable relief, civil penalties, and attorneys’ fees and costs.

CLAIMS ON BEHALF OF THE NEVADA SUBCLASS

COUNT 53

NEVADA DECEPTIVE TRADE PRACTICES ACT

Nev. Rev. Stat. Ann. §§ 598.0903, et seq.

944. Nevada Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Nevada Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

945. Marriott advertised, offered, or sold goods or services in Nevada and engaged in trade or commerce directly or indirectly affecting the people of Nevada.

946. Marriott engaged in deceptive trade practices in the course of its business or occupation, in violation of Nev. Rev. Stat. §§ 598.0915 and 598.0923, including:

a. Knowingly making a false representation as to the characteristics, uses, and benefits of goods or services for sale in violation of Nev. Rev. Stat. § 598.0915(5);

b. Representing that goods or services for sale are of a particular standard, quality, or grade when Marriott knew or should have known that they are of another standard, quality, or grade in violation of Nev. Rev. Stat. § 598.0915(7);

c. Advertising goods or services with intent not to sell them as advertised in violation of Nev. Rev. Stat. § 598.0915(9);

d. Failing to disclose a material fact in connection with the sale of goods or services in violation of Nev. Rev. Stat. § 598.0923(A)(2); and

e. Violating state and federal statutes or regulations relating to the sale of goods or services in violation of Nev. Rev. Stat. § 598.0923(A)(3).

947. Marriott’s deceptive trade practices in the course of its business or occupation include:

a. Failing to implement and maintain reasonable security and privacy measures

to protect Plaintiff and Nevada Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nevada Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Nevada's data security statute, Nev. Rev. Stat. § 603A.210, which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Nevada Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nevada Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; and Nevada's data security statute, Nev. Rev. Stat. § 603A.210;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Nevada Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Nevada's data security statute, Nev. Rev. Stat. § 603A.210.

948. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect

the confidentiality of consumers' Personal Information.

949. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as secure and was trusted with sensitive and valuable Personal Information regarding millions of consumers, including Plaintiff and the Nevada Subclass.

950. Marriott accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public.

951. Plaintiff and the Nevada Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

952. Marriott acted intentionally, knowingly, and maliciously to violate Nevada's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Nevada Subclass members' rights. Past breaches put Marriott on notice that its security and privacy protections were inadequate.

953. As a direct and proximate result of Marriott's deceptive trade practices, Plaintiff and Nevada Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

954. Plaintiff and Nevada Subclass members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEW JERSEY SUBCLASS

COUNT 54

NEW JERSEY CUSTOMER SECURITY BREACH DISCLOSURE ACT

N.J. Stat. Ann. §§ 56:8-163, et seq.

955. New Jersey Plaintiffs identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the New Jersey Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

956. Marriott is a business that compiles or maintains computerized records that include Personal Information on behalf of another business under N.J. Stat. Ann. § 56:8-163(b).

957. Plaintiffs’ and New Jersey Subclass members’ Personal Information includes Personal Information covered under N.J. Stat. Ann. §§ 56:8-163, et seq.

958. Under N.J. Stat. Ann. § 56:8-163(b), “[a]ny business . . . that compiles or maintains computerized records that include Personal Information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers . . . of any breach of security of the computerized records immediately following discovery, if the Personal Information was, or is reasonably believed to have been, accessed by an unauthorized person.”

959. Because Marriott discovered a breach of its security system in which Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, Marriott had an obligation to disclose the Breach in a timely and accurate fashion as mandated under N.J. Stat. Ann. §§ 56:8-163, et seq.

960. By failing to disclose the Breach in a timely and accurate manner, Marriott violated N.J. Stat. Ann. § 56:8-163(b).

961. As a direct and proximate result of Marriott’s violations of N.J. Stat. Ann. § 56:8-163(b), Plaintiff and New Jersey Subclass members suffered the damages described above.

962. Plaintiffs and New Jersey Subclass members seek relief under N.J. Stat. Ann. § 56:8-19, including treble damages, attorneys' fees and costs, and injunctive relief.

COUNT 55

NEW JERSEY CONSUMER FRAUD ACT

N.J. Stat. Ann. §§ 56:8-1, et seq.

963. New Jersey Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the New Jersey Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

964. Marriott is a "person," as defined by N.J. Stat. Ann. § 56:8-1(d).

965. Marriott sells "merchandise," as defined by N.J. Stat. Ann. § 56:8-1(c) & (e).

966. The New Jersey Consumer Fraud Act, N.J. Stat. §§ 56:8-1, et seq., prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

967. Marriott's unconscionable and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and New Jersey Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and New Jersey Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause

of the Marriott data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and New Jersey Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and New Jersey Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and New Jersey Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

968. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

969. Marriott intended to mislead Plaintiff and New Jersey Subclass members and induce them to rely on its misrepresentations and omissions.

970. Marriott acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiffs and New Jersey Subclass members' rights. Past breaches put Marriott on notice that its security and privacy protections were inadequate.

971. As a direct and proximate result of Marriott's unconscionable and deceptive practices, Plaintiffs and New Jersey Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages,

including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

972. Plaintiffs and New Jersey Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS

COUNT 56

INFORMATION SECURITY BREACH AND NOTIFICATION ACT

N.Y. Gen. Bus. Law § 899-aa

973. New York Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the New York Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

974. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by N.Y. Gen. Bus. Law § 899-aa(1)(a).

975. Marriott also maintains computerized data that includes Personal Information which Marriott does not own. Accordingly, it is subject to N.Y. Gen. Bus. Law §§ 899- aa(2) and (3).

976. Plaintiffs' and New York Subclass members' Personal Information includes Personal Information covered by N.Y. Gen. Bus. Law § 899-aa(1)(b).

977. Marriott is required to give immediate notice of a breach of security of a data system to owners of Personal Information which Marriott does not own, including Plaintiffs and New York Subclass members, pursuant to N.Y. Gen. Bus. Law § 899-aa(3).

978. Marriott is required to accurately notify Plaintiffs and Montana Subclass members if it discovers a security breach, or receives notice of a security breach which may have compromised Personal Information which Marriott owns or licenses, in the most expedient time

possible and without unreasonable delay under N.Y. Gen. Bus. Law § 899-aa(2).

979. By failing to disclose the Breach in a timely and accurate manner, Marriott violated N.Y. Gen. Bus. Law §§ 899-aa(2) and (3).

980. As a direct and proximate result of Marriott's violations of N.Y. Gen. Bus. Law §§ 899-aa(2) and (3), Plaintiffs and New York Subclass members suffered damages, as described above.

981. Plaintiffs and New York Subclass members seek relief under N.Y. Gen. Bus. Law § 899-aa(6)(b), including actual damages and injunctive relief.

COUNT 57

NEW YORK GENERAL BUSINESS LAW

N.Y. Gen. Bus. Law §§ 349, et seq.

982. New York Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the New York Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

983. Marriott engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and New York Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause

of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and New York Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and New York Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and New York Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

984. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

985. Marriott acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiffs and New York Subclass members' rights. Past breaches put Marriott on notice that its security and privacy protections were inadequate.

986. As a direct and proximate result of Marriott's deceptive and unlawful acts and practices, Plaintiffs and New York Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial

accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

987. Marriott's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the millions of New Yorkers affected by the Breach.

988. The above deceptive and unlawful practices and acts by Marriott caused substantial injury to Plaintiffs and New York Subclass members that they could not reasonably avoid.

989. Plaintiffs and New York Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of \$50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

CLAIMS ON BEHALF OF THE NORTH CAROLINA SUBCLASS

COUNT 58

NORTH CAROLINA IDENTITY THEFT PROTECTION ACT

N.C. Gen. Stat. §§ 75-60, et seq.

990. North Carolina Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

991. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by N.C. Gen. Stat. § 75-61(1).

992. Plaintiffs and North Carolina Subclass members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

993. Marriott is required to accurately notify Plaintiffs and North Carolina Subclass members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without unreasonable delay under N.C. Gen. Stat. § 75-65.

994. Plaintiffs' and North Carolina Subclass members' PII includes Personal Information as covered under N.C. Gen. Stat. § 75-61(10).

995. Because Marriott discovered a security breach and had notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), Marriott had an obligation to disclose the Breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. § 75-65.

996. By failing to disclose the Breach in a timely and accurate manner, Marriott violated N.C. Gen. Stat. § 75-65.

997. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. Art. 2A § 75-1.1.

998. As a direct and proximate result of Marriott's violations of N.C. Gen. Stat. § 75-65, Plaintiffs and North Carolina Subclass members suffered damages, as described above.

999. Plaintiffs and North Carolina Subclass members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorney's fees.

COUNT 59

NORTH CAROLINA UNFAIR TRADE PRACTICES ACT

N.C. Gen. Stat. Ann. §§ 75-1.1, et seq.

1000. North Carolina Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

1001. Marriott advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

1002. Marriott engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and North Carolina Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and North Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and North Carolina Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and North Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and North Carolina Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and North Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1003. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect

the confidentiality of consumers' Personal Information.

1004. Marriott intended to mislead Plaintiffs and North Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

1005. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as secure and was trusted with sensitive and valuable Personal Information regarding millions of consumers, including Plaintiffs and the North Carolina Subclass.

1006. Marriott accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public.

1007. Plaintiffs and the North Carolina Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

1008. Marriott acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiffs and North Carolina Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

1009. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiffs and North Carolina Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1010. Marriott's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

1011. Plaintiffs and North Carolina Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE OHIO SUBCLASS

COUNT 60

OHIO CONSUMER SALES PRACTICES ACT

Ohio Rev. Code §§ 1345.01, et seq.

1012. Ohio Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Ohio Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

1013. Plaintiffs and Ohio Subclass members are "persons," as defined by Ohio Rev. Code § 1345.01(B).

1014. Marriott was a "supplier" engaged in "consumer transactions," as defined by Ohio Rev. Code §§ 1345.01(A) & (C).

1015. Marriott advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

1016. Marriott engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code §§ 1345.02, including:

a. Marriott represented that its goods, services, and intangibles had performance characteristics, uses, and benefits that it did not have, in violation of Ohio Rev. Code § 1345.02(B)(1); and

b. Marriott represented that its goods, services, and intangibles were of a particular standard or quality when they were not, in violation of Ohio Rev. Code § 1345(B)(2).

1017. Marriott engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code Ann. § 1345.03, including:

a. Knowingly taking advantage of the inability of Plaintiffs and the Ohio Subclass to reasonably protect their interest because of their ignorance of the issues discussed herein (Ohio Rev. Code Ann. § 1345.03(B)(1)); and

b. Requiring Plaintiff and the Ohio Subclass to enter into a consumer transaction on terms that Marriott knew were substantially one-sided in favor of Marriott (Ohio Rev. Code Ann. § 1345.03(B)(5)).

1018. Marriott's unfair, deceptive, and unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Ohio Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Ohio Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Ohio Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not

comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1019. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1020. Marriott intended to mislead Plaintiffs and Ohio Subclass members and induce them to rely on its misrepresentations and omissions.

1021. Marriott acted intentionally, knowingly, and maliciously to violate Ohio's Consumer Sales Practices Act, and recklessly disregarded Plaintiffs and Ohio Subclass members' rights. Past breaches put Marriott on notice that its security and privacy protections were inadequate.

1022. Marriott's unfair, deceptive, and unconscionable acts and practices complained of herein affected the public interest, including the millions of Ohioans affected by the Breach.

1023. As a direct and proximate result of Marriott's unfair, deceptive, and unconscionable acts and practices, Plaintiff and Ohio Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1024. Plaintiffs and the Ohio Subclass members seek all monetary and nonmonetary relief allowed by law, including declaratory and injunctive relief, the greater of actual and treble damages or statutory damages, attorneys' fees and costs, and any other appropriate relief.

COUNT 61

OHIO DECEPTIVE TRADE PRACTICES ACT

Ohio Rev. Code §§ 4165.01, et seq.

1025. Ohio Plaintiffs identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the Ohio Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

1026. Marriott, Plaintiffs, and Ohio Subclass members are all “persons,” as defined by Ohio Rev. Code § 4165.01(D).

1027. Marriott advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

1028. Marriott engaged in deceptive trade practices in the course of its business and vocation, in violation of Ohio Rev. Code § 4165.02, including:

a. Representing that its goods and services have characteristics, uses, benefits, or qualities that they do not have, in violation of Ohio Rev. Code § 4165.02(A)(7);

b. Representing that its goods and services are of a particular standard or quality when they are of another, in violation of Ohio Rev. Code § 4165.02(A)(9); and

c. Advertising its goods and services with intent not to sell them as advertise, in violation of Ohio Rev. Code § 4165.02(A)(11).

1029. Marriott’s deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Ohio Subclass members’ Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Ohio Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Ohio Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1030. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1031. Marriott intended to mislead Plaintiffs and Ohio Subclass members and induce them to rely on its misrepresentations and omissions.

1032. Marriott acted intentionally, knowingly, and maliciously to violate Ohio's Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs and Ohio Subclass members' rights. Past breaches put Marriott on notice that its security and privacy protections were inadequate.

1033. As a direct and proximate result of Marriott's deceptive trade practices, Plaintiffs

and Ohio Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1034. Plaintiffs and Ohio Subclass members seek all monetary and nonmonetary relief allowed by law, including injunctive relief, actual damages, attorneys' fees, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE OKLAHOMA SUBCLASS

COUNT 62

OKLAHOMA CONSUMER PROTECTION ACT

Okla. Stat. Tit. 15, §§ 751, et seq.

1035. Oklahoma Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Oklahoma Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

1036. Marriott is a "person," as meant by Okla. Stat. tit. 15, § 752(1).

1037. Marriott's advertisements, offers of sales, sales, and distribution of goods, services, and other things of value constituted "consumer transactions" as meant by Okla. Stat. tit. 15, § 752(2).

1038. Marriott, in the course of its business, engaged in unlawful practices in violation of Okla. Stat. tit. 15, § 753, including the following:

a. Making false representations, knowingly or with reason to know, as to the characteristics, uses, and benefits of the subjects of its consumer transactions, in violation of Okla. Stat. tit. 15, § 753(5);

b. Representing, knowingly or with reason to know, that the subjects of its

consumer transactions were of a particular standard when they were of another, in violation of Okla. Stat. tit 15, § 753(7);

c. Advertising, knowingly or with reason to know, the subjects of its consumer transactions with intent not to sell as advertised, in violation of Okla. Stat. tit 15, § 753 (8);

d. Committing unfair trade practices that offend established public policy and was immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers as defined by section 752(14), in violation of Okla. Stat. tit. 15, § 753(20); and

e. Committing deceptive trade practices that deceived or could reasonably be expected to deceive or mislead a person to the detriment of that person as defined by section 752(13), in violation of Okla. Stat. tit. 15, § 753(20).

1039. Marriott's unlawful practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Oklahoma Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Oklahoma Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Oklahoma Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Oklahoma Subclass members' Personal

Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Oklahoma Subclass members' Personal Information; and

g Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Oklahoma Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1040. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1041. Marriott intended to mislead Plaintiffs and Oklahoma Subclass members and induce them to rely on its misrepresentations and omissions.

1042. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as secure and was trusted with sensitive and valuable Personal Information regarding millions of consumers, including Plaintiffs and the Oklahoma Subclass.

1043. Marriott accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public.

1044. Plaintiffs and the Oklahoma Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

1045. The above unlawful practices and acts by Marriott were immoral, unethical, oppressive, unscrupulous, and substantially injurious. These acts caused substantial injury to Plaintiffs and Oklahoma Subclass members.

1046. Marriott acted intentionally, knowingly, and maliciously to violate Oklahoma's Consumer Protection Act, and recklessly disregarded Plaintiffs and Oklahoma Subclass members' rights. Past breaches put Marriott on notice that its security and privacy protections were inadequate.

1047. As a direct and proximate result of Marriott's unlawful practices, Plaintiffs and Oklahoma Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1048. Plaintiffs and Oklahoma Subclass members seek all monetary and nonmonetary relief allowed by law, including actual damages, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE OREGON SUBCLASS

COUNT 63

OREGON CONSUMER IDENTITY THEFT PROTECTION ACT

Or. Rev. Stat. §§ 646A.604(1), et seq.

1049. Oregon Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Oregon Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

1050. Marriott is a business that maintains records which contain Personal Information, within the meaning of Or. Rev. Stat. § 646A.622(1), about Plaintiffs and Oregon Subclass members.

1051. Pursuant to Or. Rev. Stat. § 646A.622(1), a business "that maintains records which contain Personal Information" of an Oregon resident "shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use,

modification or disclosure.”

1052. Marriott violated Or. Rev. Stat. § 646A.622(1) by failing to implement reasonable measures to protect Plaintiffs’ and Oregon Subclass members’ Personal Information.

1053. Marriott is a business that owns, maintains, or otherwise possesses data that includes consumers Personal Information as defined by Or. Rev. Stat. § 646A.604(1).

1054. Plaintiffs’ and Oregon Subclass members’ PII includes Personal Information as covered under Or. Rev. Stat. § 646A.604(1).

1055. Marriott is required to accurately notify Plaintiffs and Oregon Subclass members if it becomes aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Or. Rev. Stat. § 646A.604(1).

1056. Because Marriott discovered a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Or. Rev. Stat. § 646A.604(1).

1057. By failing to disclose the Breach in a timely and accurate manner, Marriott violated Or. Rev. Stat. § 646A.604(1).

1058. Pursuant to Or. Rev. Stat. § 646A.604(9), violations of Or. Rev. Stat. §§ 646A.604(1) and 646A.622(1) are unlawful practices under Or. Rev. Stat. § 646.607.

1059. As a direct and proximate result of Marriott’s violations of Or. Rev. Stat. §§ 646A.604(1) and 646A.622(1), Plaintiff and Oregon Subclass members suffered damages, as described above.

1060. Plaintiffs and Oregon Subclass members seek relief under Or. Rev. Stat. § 646.638, including actual damages, punitive damages, and injunctive relief.

COUNT 64

OREGON UNLAWFUL TRADE PRACTICES ACT

Or. Rev. Stat. §§ 646.608, et seq.

1061. Oregon Plaintiffs identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the Oregon Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

1062. Marriott is a “person,” as defined by Or. Rev. Stat. § 646.605(4).

1063. Marriott engaged in the sale of “goods and services,” as defined by Or. Rev. Stat. § 646.605(6)(a).

1064. Marriott sold “goods or services,” as defined by Or. Rev. Stat. § 646.605(6)(a).

1065. Marriott advertised, offered, or sold goods or services in Oregon and engaged in trade or commerce directly or indirectly affecting the people of Oregon.

1066. Marriott engaged in unlawful practices in the course of its business and occupation, in violation of Or. Rev. Stat. § 646.608, included the following:

a. Representing that its goods and services have approval, characteristics, uses, benefits, and qualities that they do not have, in violation of Or. Rev. Stat. § 646.608(1)(e);

b. Representing that its goods and services are of a particular standard or quality if they are of another, in violation of Or. Rev. Stat. § 646.608(1)(g);

c. Advertising its goods or services with intent not to provide them as advertised, in violation of Or. Rev. Stat. § 646.608(1)(i); and

d. Concurrent with tender or delivery of its goods and services, failing to disclose any known material defect, in violation of Or. Rev. Stat. § 646.608(1)(t).

1067. Marriott’s unlawful practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Oregon Subclass members’ Personal Information, which was a direct and

proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Oregon Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, et seq., which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Oregon Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Oregon Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, et seq.;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Oregon Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Oregon Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, et seq.

1068. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect

the confidentiality of consumers' Personal Information.

1069. Marriott intended to mislead Plaintiffs and Oregon Subclass members and induce them to rely on its misrepresentations and omissions.

1070. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as secure and was trusted with sensitive and valuable Personal Information regarding millions of consumers, including Plaintiffs and the Oregon Subclass.

1071. Marriott accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public.

1072. Plaintiffs and the Oregon Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

1073. Marriott acted intentionally, knowingly, and maliciously to violate Oregon's Unlawful Trade Practices Act, and recklessly disregarded Plaintiffs and Oregon Subclass members' rights. Past breaches put Marriott on notice that its security and privacy protections were inadequate.

1074. As a direct and proximate result of Marriott's unlawful practices, Plaintiffs and Oregon Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1075. Plaintiffs and Oregon Subclass members seek all monetary and nonmonetary relief allowed by law, including equitable relief, actual damages or statutory damages of \$200 per violation (whichever is greater), punitive damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE PENNSYLVANIA SUBCLASS

COUNT 65

PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW

73 Pa. Cons. Stat. §§ 201-2 & 201-3, et seq.

1076. Pennsylvania Plaintiffs identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the Pennsylvania Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

1077. Marriott is a “person”, as meant by 73 Pa. Cons. Stat. § 201-2(2).

1078. Plaintiffs and Pennsylvania Subclass members purchased goods and services in “trade” and “commerce,” as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

1079. Marriott Pennsylvania engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including the following:

- a. Representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));
- b. Representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201-2(4)(vii)); and
- c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

1080. Marriott’s unfair or deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Pennsylvania Subclass members’ Personal Information, which was a direct and proximate cause of the Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate

identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Pennsylvania Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Pennsylvania Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Pennsylvania Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Pennsylvania Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Pennsylvania Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1081. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1082. Marriott intended to mislead Plaintiffs and Pennsylvania Subclass members and induce them to rely on its misrepresentations and omissions.

1083. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business

and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as secure and was trusted with sensitive and valuable Personal Information regarding millions of consumers, including Plaintiffs and the Pennsylvania Subclass.

1084. Marriott accepted the responsibility of being a “steward of data” while keeping the inadequate state of its security controls secret from the public.

1085. Plaintiffs and the Pennsylvania Subclass members acted reasonably in relying on Marriott’s misrepresentations and omissions, the truth of which they could not have discovered.

1086. Marriott acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiffs and Pennsylvania Subclass members’ rights. Marriott’s numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1087. As a direct and proximate result of Marriott’s unfair methods of competition and unfair or deceptive acts or practices and Plaintiffs’ and the Pennsylvania Subclass’ reliance on them, Plaintiffs and Pennsylvania Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1088. Plaintiffs and Pennsylvania Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of \$100 (whichever is greater), treble damages, attorneys’ fees and costs, and any additional relief the Court deems necessary or proper.

CLAIMS ON BEHALF OF THE RHODE ISLAND SUBCLASS

COUNT 66

RHODE ISLAND DECEPTIVE TRADE PRACTICES ACT,

R.I. Gen. Laws §§ 6-13.1, et seq.

1089. Rhode Island Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Rhode Island Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

1090. Plaintiff and Rhode Island Subclass members are each a “person,” as defined by R.I. Gen. Laws § 6-13.1-1(3).

1091. Plaintiff and Rhode Island Subclass members purchased goods and services for personal, family, or household purposes.

1092. Marriott advertised, offered, or sold goods or services in Rhode Island and engaged in trade or commerce directly or indirectly affecting the people of Rhode Island, as defined by R.I. Gen. Laws § 6-13.1-1(5).

1093. Marriott engaged in unfair and deceptive acts and practices, in violation of R.I. Gen. Laws § 6-13.1-2, including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have (R.I. Gen. Laws § 6-13.1-52(6)(v));

b. Representing that its goods and services are of a particular standard or quality when they are of another (R.I. Gen. Laws § 6-13.1-52(6)(vii));

c. Advertising goods or services with intent not to sell them as advertised (R.I. Gen. Laws § 6-13.1-52(6)(ix));

d. Engaging in any other conduct that similarly creates a likelihood of confusion or misunderstanding (R.I. Gen. Laws § 6-13.1-52(6)(xii));

e. Engaging in any act or practice that is unfair or deceptive to the consumer

(R.I. Gen. Laws § 6-13.1-52(6)(xiii)); and

f. Using other methods, acts, and practices that mislead or deceive members of the public in a material respect (R.I. Gen. Laws §6-13.1-52(6)(xiv)).

1094. Marriott's unfair and deceptive acts include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Rhode Island Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Rhode Island Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2, which was a direct and proximate cause of the Marriott data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Rhode Island Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Rhode Island Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Rhode Island Subclass members' Personal Information; and

g Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Rhode Island Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2.

1095. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1096. Marriott intended to mislead Plaintiff and Rhode Island Subclass members and induce them to rely on its misrepresentations and omissions.

1097. Marriott acted intentionally, knowingly, and maliciously to violate Rhode Island's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Rhode Island Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

1098. As a direct and proximate result of Marriott's unfair and deceptive acts, Plaintiff and Rhode Island Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1099. Plaintiff and Rhode Island Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of \$200 per Subclass Member (whichever is greater), punitive damages, injunctive relief, other equitable relief, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE SOUTH CAROLINA SUBCLASS

COUNT 67

SOUTH CAROLINA DATA BREACH SECURITY ACT

S.C. Code Ann. §§ 39-1-90, et seq.

1100. South Carolina Plaintiffs identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the South Carolina Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

1101. Marriott is a business that owns or licenses computerized data or other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A).

1102. Plaintiffs’ and South Carolina Subclass members’ PII includes personal identifying information as covered under S.C. Code Ann. § 39-1-90(D)(3).

1103. Marriott is required to accurately notify Plaintiffs and South Carolina Subclass members following discovery or notification of a breach of its data security system if Personal Information that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, in the most expedient time possible and without unreasonable delay under S.C. Code Ann. § 39-1-90(A).

1104. Because Marriott discovered a breach of its data security system in which Personal Information that was not rendered unusable through encryption, redaction, or other methods, was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, Marriott had an obligation to disclose the Breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A).

1105. By failing to disclose the Breach in a timely and accurate manner, Marriott violated S.C. Code Ann. § 39-1-90(A).

1106. As a direct and proximate result of Marriott’s violations of S.C. Code Ann. § 39-1-

90(A), Plaintiffs and South Carolina Subclass members suffered damages, as described above.

1107. Plaintiffs and South Carolina Subclass members seek relief under S.C. Code Ann. § 39-1-90(G), including actual damages and injunctive relief.

COUNT 68

SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT

S.C. Code Ann. §§ 39-5-10, et seq.

1108. South Carolina Plaintiffs identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the South Carolina Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

1109. Marriott is a “person,” as defined by S.C. Code Ann. § 39-5-10(a).

1110. South Carolina’s Unfair Trade Practices Act (SC UTPA) prohibits “unfair or deceptive acts or practices in the conduct of any trade or commerce.” S.C. Code Ann. § 39-5-20.

1111. Marriott advertised, offered, or sold goods or services in South Carolina and engaged in trade or commerce directly or indirectly affecting the people of South Carolina, as defined by S.C. Code Ann. § 39-5-10(b).

1112. Marriott engaged in unfair and deceptive acts and practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and South Carolina Subclass members’ Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and South Carolina Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause

of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and South Carolina Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and South Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and South Carolina Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and South Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1113. Marriott's acts and practices had, and continue to have, the tendency or capacity to deceive.

1114. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1115. Marriott intended to mislead Plaintiffs and South Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

1116. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as secure and was trusted with sensitive and valuable Personal

Information regarding millions of consumers, including Plaintiffs and the South Carolina Subclass.

1117. Marriott accepted the responsibility of being a “steward of data” while keeping the inadequate state of its security controls secret from the public.

1118. Plaintiffs and the South Carolina Subclass members acted reasonably in relying on Marriott’s misrepresentations and omissions, the truth of which they could not have discovered.

1119. Marriott had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensiveness of the Personal Information in its possession, and the generally accepted professional standards.

1120. Such a duty is also implied by law due to the nature of the relationship between consumers—including Plaintiffs and the South Carolina Subclass—and Marriott, because consumers are unable to fully protect their interests with regard to the Personal Information in Marriott’s possession, and place trust and confidence in Marriott.

1121. Marriott’s duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and the South Carolina Subclass that contradicted these representations.

1122. Marriott’s business acts and practices offend an established public policy, or are immoral, unethical, or oppressive. Marriott’s acts and practices offend established public policies that seek to protect consumers’ Personal Information and ensure that entities entrusted with Personal Information use appropriate security measures. These public policies are reflected in laws such as the FTC Act, 15 U.S.C. § 45 and the South Carolina Data Breach Security Act, S.C. Code § 39-1-90, et seq.

1123. Marriott's failure to implement and maintain reasonable security measures was immoral, unethical, or oppressive in light of Marriott's long history of inadequate data security and previous data breaches; the sensitivity and extensiveness of Personal Information in its possession.

1124. Marriott's unfair and deceptive acts or practices adversely affected the public interest because such acts or practices have the potential for repetition; Marriott engages in such acts or practices as a general rule; and such acts or practices impact the public at large.

1125. Marriott's unfair and deceptive acts or practices have the potential for repetition because the same kinds of actions occurred in the past, including numerous past data breaches, thus making it likely that these acts or practices will continue to occur if left undeterred. Additionally, Marriott's policies and procedures, such as its security practices, create the potential for recurrence of the complained-of business acts and practices.

1126. Marriott's violations present a continuing risk to Plaintiffs and South Carolina Subclass members as well as to the general public.

1127. Marriott intended to mislead Plaintiffs and South Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

1128. Marriott acted intentionally, knowingly, and maliciously to violate South Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiffs and South Carolina Subclass members' rights. Past data breaches put it on notice that its security and privacy protections were inadequate. In light of this conduct, punitive damages would serve the interest of society in punishing and warning others not to engage in such conduct, and would deter Marriott and others from committing similar conduct in the future.

1129. As a direct and proximate result of Marriott's unfair and deceptive acts or practices, Plaintiffs and South Carolina Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for

fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1130. Plaintiffs and South Carolina Subclass members seek all monetary and non-monetary relief allowed by law, including damages for their economic losses; treble damages; punitive damages; injunctive relief; and reasonable attorneys' fees.

CLAIMS ON BEHALF OF THE TENNESSEE SUBCLASS

COUNT 69

TENNESSEE PERSONAL CONSUMER INFORMATION RELEASE ACT

Tenn. Code Ann. §§ 47-18-2107, et seq.

1131. Tennessee Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Tennessee Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

1132. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Tenn. Code Ann. § 47-18-2107(a)(2).

1133. Plaintiffs' and Tennessee Subclass members' Personal Information include Personal Information as covered under Tenn. Code Ann. § 47-18- 2107(a)(3)(A).

1134. Marriott is required to accurately notify Plaintiffs and Tennessee Subclass members following discovery or notification of a breach of its data security system in which unencrypted Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person, in the most expedient time possible and without unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

1135. Because Marriott discovered a breach of its security system in which unencrypted Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person, Marriott had an obligation to disclose the Breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

1136. By failing to disclose the Breach in a timely and accurate manner, Marriott violated Tenn. Code Ann. § 47-18-2107(b).

1137. As a direct and proximate result of Marriott's violations of Tenn. Code Ann. § 47-18-2107(b), Plaintiff and Tennessee Subclass members suffered damages, as described above.

1138. Plaintiffs and Tennessee Subclass members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), and 47-18-2104(f), including actual damages, injunctive relief, and treble damages.

COUNT 70

TENNESSEE CONSUMER PROTECTION ACT

Tenn. Code Ann. §§ 47-18-101, et seq.

1139. Tennessee Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Tennessee Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

1140. Marriott is a "person," as defined by Tenn. Code § 47-18-103(13).

1141. Plaintiffs and Tennessee Subclass members are "consumers," as meant by Tenn. Code § 47-18-103(2).

1142. Marriott advertised and sold "goods" or "services" in "consumer transaction[s]," as defined by Tenn. Code §§ 47-18-103(7), (18) & (19).

1143. Marriott advertised, offered, or sold goods or services in Tennessee and engaged in trade or commerce directly or indirectly affecting the people of Tennessee, as defined by Tenn. Code §§ 47-18-103(7), (18) & (19). And Marriott's acts or practices affected the conduct of trade or commerce, under Tenn. Code § 47-18-104.

1144. Marriott's unfair and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Tennessee Subclass members' Personal Information, which was a direct

and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Tennessee Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Tennessee Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Tennessee Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Tennessee Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1145. Marriott intended to mislead Plaintiff and Tennessee Subclass members and induce them to rely on its misrepresentations and omissions.

1146. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect

the confidentiality of consumers' Personal Information.

1147. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as secure and was trusted with sensitive and valuable Personal Information regarding millions of consumers including Plaintiffs and the Tennessee Subclass.

1148. Marriott accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public.

1149. Plaintiff and the Tennessee Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

1150. Marriott had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensiveness of the Personal Information in its possession, and the generally accepted professional standards. This duty arose because members of the public, including Plaintiffs and the Tennessee Subclass, repose a trust and confidence in Marriott. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiffs and the Tennessee Subclass, and Marriott because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott.

1151. Marriott's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and the Tennessee Subclass that contradicted these representations.

1152. Marriott's "unfair" acts and practices caused or were likely to cause substantial

injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1153. The injury to consumers was and is substantial because it was nontrivial and non-speculative, and involved a monetary injury and/or an unwarranted risk to the safety of their Personal Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1154. Consumers could not have reasonably avoided injury because Marriott's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Marriott created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1155. Marriott's inadequate data security had no countervailing benefit to consumers or to competition.

1156. By misrepresenting and omitting material facts about its data security and failing to comply with its common law and statutory duties pertaining to data security (including its duties under the FTC Act), Marriott violated the following provisions of Tenn. Code § 47-18-104(b):

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;
- b. Representing that goods or services are of a particular standard, quality or grade, if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised; and
- d. Representing that a consumer transaction confers or involves rights, remedies or obligations that it does not have or involve.

1157. Marriott acted intentionally, knowingly, and maliciously to violate Tennessee's

Consumer Protection Act, and recklessly disregarded Plaintiffs and Tennessee Subclass members' rights. Past breaches put Marriott on notice that its security and privacy protections were inadequate.

1158. As a direct and proximate result of Marriott's unfair and deceptive acts or practices, Plaintiffs and Tennessee Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1159. Marriott's violations present a continuing risk to Plaintiffs and Tennessee Subclass members as well as to the general public.

1160. Plaintiffs and Tennessee Subclass members seek all monetary and nonmonetary relief allowed by law, including injunctive relief, actual damages, treble damages for each willful or knowing violation, attorneys' fees and costs, and any other relief that is necessary and proper.

CLAIMS ON BEHALF OF THE TEXAS SUBCLASS

COUNT 71

DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT

Tex. Bus. & Com. Code §§ 17.41, et seq.

1161. Texas Plaintiffs identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Texas Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

1162. Marriott is a "person," as defined by Tex. Bus. & Com. Code § 17.45(3).

1163. Plaintiffs and the Texas Subclass members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

1164. Marriott advertised, offered, or sold goods or services in Texas and engaged in

trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

1165. Marriott engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;
- b. Representing that goods or services are of a particular standard, quality or grade, if they are of another; and
- c. Advertising goods or services with intent not to sell them as advertised.

1166. Marriott's false, misleading, and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Texas Subclass members' Personal Information, which was a direct and proximate cause of the Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Texas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Texas Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Texas Subclass members' Personal

Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Texas's data security statute, Tex. Bus. & Com. Code § 521.052;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Texas Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Texas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Texas's data security statute, Tex. Bus. & Com. Code § 521.052.

1167. Marriott intended to mislead Plaintiffs and Texas Subclass members and induce them to rely on its misrepresentations and omissions.

1168. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1169. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as secure and was trusted with sensitive and valuable Personal Information regarding millions of consumers, including Plaintiffs and the Texas Subclass.

1170. Marriott accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public.

1171. Plaintiffs and the Texas Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

1172. Marriott had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensiveness of the Personal Information in its possession, and the generally

accepted professional standards. This duty arose because members of the public, including Plaintiffs and the Texas Subclass, repose a trust and confidence in Marriott. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiffs and the Texas Subclass, and Marriott because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott.

1173. Marriott's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and the Texas Subclass that contradicted these representations.

1174. Marriott engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Marriott engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

1175. Consumers, including Plaintiffs and Texas Subclass members, lacked knowledge about deficiencies in Marriott's data security because this information was known exclusively by Marriott. Consumers also lacked the ability, experience, or capacity to secure the Personal Information in Marriott's possession or to fully protect their interests with regard to their data. Plaintiffs and Texas Subclass members lack expertise in information security matters and do not have access to Marriott's systems in order to evaluate its security controls. Marriott took advantage of its special skill and access to Personal Information to hide its inability to protect the security and confidentiality of Plaintiffs and Texas Subclass members' Personal Information.

1176. Marriott intended to take advantage of consumers' lack of knowledge, ability,

experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from Marriott's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Marriott data breach, which resulted from Marriott's unconscionable business acts and practices, exposed Plaintiffs and Texas Subclass members to a wholly unwarranted risk to the safety of their Personal Information and the security of their identity or credit, and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiffs and Texas Subclass members cannot mitigate this unfairness because they cannot undo the data breach.

1177. Marriott acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiffs and Texas Subclass members' rights. Marriott's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1178. As a direct and proximate result of Marriott's unconscionable and deceptive acts or practices, Plaintiffs and Texas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information. Marriott's unconscionable and deceptive acts or practices were a producing cause of Plaintiffs' and Texas Subclass members' injuries, ascertainable losses, economic damages, and non-economic damages, including their mental anguish.

1179. Marriott's violations present a continuing risk to Plaintiffs and Texas Subclass members as well as to the general public.

1180. Plaintiffs and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for each act committed intentionally or knowingly; court costs; reasonably and necessary attorneys'

fees; injunctive relief; and any other relief which the court deems proper.

CLAIMS ON BEHALF OF THE UTAH SUBCLASS

COUNT 72

UTAH CONSUMER SALES PRACTICES ACT,

Utah Code §§ 13-11-1, et seq.

1181. Utah Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Utah Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

1182. Defendant is a “person,” as defined by Utah Code § 13-11-1(5).

1183. Defendant is a “supplier,” as defined by Utah Code § 13-11-1(6), because it regularly solicits, engages in, or enforces “consumer transactions,” as defined by Utah Code § 13-11-1(2).

1184. Defendant engaged in deceptive and unconscionable acts and practices in connection with consumer transactions, in violation of Utah Code § 13-11-4 and Utah Code § 13-11-5, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Utah Subclass members’ Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Utah Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Utah Protection of Personal Information Act, Utah Code § 13-44-201, which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Utah Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Utah Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Utah Protection of Personal Information Act, Utah Code § 13-44-201;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; and the Utah Protection of Personal Information Act, Utah Code § 13-44-201.

1185. Defendant intended to mislead Plaintiff and Utah Subclass members and induce them to rely on its misrepresentations and omissions.

1186. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Personal Information.

1187. Had Defendant disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant held itself out as secure and was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Utah Subclass.

1188. Defendant accepted the responsibility of being a "steward of data" while keeping

the inadequate state of its security controls secret from the public.

1189. Plaintiff and the Utah Subclass members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

1190. Defendant had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensivity of the Personal Information in its possession, and the generally accepted professional standards. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Utah Subclass, and Defendant because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendant.

1191. Defendant's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Utah Subclass that contradicted these representations.

1192. Defendant intentionally or knowingly engaged in deceptive acts or practices, violating Utah Code § 13-11-4(2) by:

- a. Indicating that the subject of a consumer transaction has sponsorship, approval, performance characteristics, accessories, uses, or benefits, if it has not;
- b. Indicating that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not;
- c. Indicating that the subject of a consumer transaction has been supplied in accordance with a previous representation, if it has not;
- d. Indicating that the subject of a consumer transaction will be supplied in

greater quantity (e.g. more data security) than the supplier intends.

1193. Defendant engaged in unconscionable acts and practices that were oppressive and led to unfair surprise, as shown in the setting, purpose, and effect of those acts and practices. Defendant's acts and practices unjustly imposed hardship on Plaintiff and the Utah Subclass by imposing on them, through no fault of their own, an increased and imminent risk of fraud and identity theft; substantial cost in time and expenses related to monitoring their financial accounts for fraudulent activity; and lost value of their Personal Information. The deficiencies in Defendant's data security, and the material misrepresentations and omissions concerning those deficiencies, led to unfair surprise to Plaintiff and the Utah Subclass when the Data Breach occurred.

1194. In addition, there was an overall imbalance in the obligations and rights imposed by the consumer transactions in question, based on the mores and industry standards of the time and place where they occurred. Societal standards required Defendant to adequately secure Personal Information in its possession. There is a substantial imbalance between the obligations and rights of consumers, such as Plaintiff and the Utah Subclass and Defendant, which has complete control over the Personal Information in its possession. Industry standards also dictate that Defendant adequately secure the Personal Information in its possession.

1195. Defendant's acts and practices were also procedurally unconscionable because consumers, including Plaintiff and the Utah Subclass, had no practicable option but to have their Personal Information stored in Defendant's systems. Defendant exploited this imbalance in power, and the asymmetry of information about its data security, to profit by inadequately securing the Personal Information in its systems.

1196. As a direct and proximate result of Defendant's unconscionable and deceptive acts or practices, Plaintiffs and Utah Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages,

including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1197. Defendant's violations present a continuing risk to Plaintiffs and Utah Subclass members as well as to the general public.

1198. Plaintiff and Utah Subclass members seek all monetary and nonmonetary relief allowed by law, including actual damages, statutory damages of \$2,000 per violation, amounts necessary to avoid unjust enrichment, under Utah Code §§ 13-11-19, et seq.; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE VIRGINIA SUBCLASS

COUNT 73

VIRGINIA PERSONAL INFORMATION BREACH NOTIFICATION ACT

Va. Code. Ann. §§ 18.2-186.6, et seq.

1199. Virginia Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Virginia Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

1200. Marriott is required to accurately notify Plaintiffs and Virginia Subclass members following discovery or notification of a breach of its data security system if unencrypted or unredacted Personal Information was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identify theft or another fraud, without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

1201. Marriott is an entity that owns or licenses computerized data that includes Personal Information as defined by Va. Code Ann. § 18.2-186.6(B).

1202. Plaintiffs' and Virginia Subclass members' PII includes Personal Information as covered under Va. Code Ann. § 18.2-186.6(A).

1203. Because Marriott discovered a breach of its security system in which unencrypted or unredacted Personal Information was or is reasonably believed to have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identify theft or another fraud, Marriott had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

1204. By failing to disclose the Breach in a timely and accurate manner, Marriott violated Va. Code Ann. § 18.2-186.6(B).

1205. As a direct and proximate result of Marriott's violations of Va. Code Ann. § 18.2-186.6(B), Plaintiffs and Virginia Subclass members suffered damages, as described above.

1206. Plaintiffs and Virginia Subclass members seek relief under Va. Code Ann. § 18.2-186.6(I), including actual damages.

COUNT 74

VIRGINIA CONSUMER PROTECTION ACT

Va. Code Ann. §§ 59.1-196, et seq.

1207. Virginia Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Virginia Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

1208. The Virginia Consumer Protection Act prohibits "[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction." Va. Code Ann. § 59.1-200(14).

1209. Marriott is a "person" as defined by Va. Code Ann. § 59.1-198.

1210. Marriott is a "supplier," as defined by Va. Code Ann. § 59.1-198.

1211. Marriott engaged in the complained-of conduct in connection with "consumer transactions" with regard to "goods" and "services," as defined by Va. Code Ann. § 59.1-198. Marriott advertised, offered, or sold goods or services used primarily for personal, family or

household purposes.

1212. Marriott engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with consumer transactions, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Virginia Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Virginia Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Virginia Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs

and Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1213. Marriott intended to mislead Plaintiffs and Virginia Subclass members and induce them to rely on its misrepresentations and omissions.

1214. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and Virginia Subclass members, about the adequacy of Marriott's computer and data security and the quality of the Marriott brand.

1215. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Marriott held itself out as secure and was trusted with sensitive and valuable Personal Information regarding millions of consumers, including Plaintiffs and the Virginia Subclass.

1216. Marriott accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public.

1217. Plaintiffs and the Virginia Subclass members acted reasonably in relying on Marriott's misrepresentations and omissions, the truth of which they could not have discovered.

1218. In Marriott had a duty to disclose these facts due to the circumstances of this case, the sensitivity and extensiveness of the Personal Information in its possession, and the generally accepted professional standards. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Virginia Subclass—and Marriott, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott.

1219. Marriott's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and the Virginia Subclass that contradicted these representations.

1220. The above-described deceptive acts and practices also violated the following provisions of VA Code § 59.1-200(A):

a. Misrepresenting that goods or services have certain quantities, characteristics, ingredients, uses, or benefits;

b. Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model; and

c. Advertising goods or services with intent not to sell them as advertised, or with intent not to sell them upon the terms advertised.

1221. Marriott acted intentionally, knowingly, and maliciously to violate Virginia's Consumer Protection Act, and recklessly disregarded Plaintiffs and Virginia Subclass members' rights. Past breaches put Marriott on notice that its security and privacy protections were inadequate. An award of punitive damages would serve to punish Marriott for its wrongdoing, and warn or deter others from engaging in similar conduct.

1222. As a direct and proximate result of Marriott's deceptive acts or practices, Plaintiffs and Virginia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1223. Marriott's violations present a continuing risk to Plaintiffs and Virginia Subclass members as well as to the general public.

1224. Plaintiffs and Virginia Subclass members seek all monetary and nonmonetary relief allowed by law, including actual damages; statutory damages in the amount of \$1,000 per violation if the conduct is found to be willful or, in the alternative, \$500 per violation; restitution, injunctive relief; punitive damages; and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE WASHINGTON SUBCLASS

COUNT 75

WASHINGTON DATA BREACH NOTICE ACT

Wash. Rev. Code §§ 19.255.010, et seq.

1225. Washington Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Washington Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

1226. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Wash. Rev. Code § 19.255.010(1).

1227. Plaintiffs' and Washington Subclass members' PII includes Personal Information as covered under Wash. Rev. Code § 19.255.010(5).

1228. Marriott is required to accurately notify Plaintiffs and Washington Subclass members following discovery or notification of the breach of its data security system if Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, in the most expedient time possible and without unreasonable delay under Wash. Rev. Code § 19.255.010(1).

1229. Because Marriott discovered a breach of its security system in which Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, Marriott had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code § 19.255.010(1).

1230. By failing to disclose the Breach in a timely and accurate manner, Marriott violated

Wash. Rev. Code § 19.255.010(1).

1231. As a direct and proximate result of Marriott's violations of Wash. Rev. Code § 19.255.010(1), Plaintiffs and Washington Subclass members suffered damages, as described above.

1232. Plaintiffs and Washington Subclass members seek relief under Wash. Rev. Code §§ 19.255.010(13)(a) and 19.255.010(13)(b), including actual damages and injunctive relief.

COUNT 76

WASHINGTON CONSUMER PROTECTION ACT

Wash. Rev. Code Ann. §§ 19.86.020, et seq.

1233. Washington Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Washington Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

1234. Marriott is a "person," as defined by Wash. Rev. Code Ann. § 19.86.010(1).

1235. Marriott advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

1236. Marriott engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Washington Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the

security and privacy of Plaintiffs and Washington Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Washington Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Washington Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Washington Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Washington Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1237. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1238. Marriott acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiffs and Washington Subclass members' rights. Past breaches put Marriott on notice that its security and privacy protections were inadequate.

1239. Marriott's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public

interest impact, and/or injured persons and had and has the capacity to injure persons. Further, its conduct affected the public interest, including the millions of Washingtonians affected by the Breach.

1240. As a direct and proximate result of Marriott's unfair methods of competition and unfair or deceptive acts or practices, Plaintiffs and Washington Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1241. Plaintiff and Washington Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE WEST VIRGINIA SUBCLASS

COUNT 77

WEST VIRGINIA CONSUMER CREDIT AND PROTECTION ACT,

W. Va. Code §§ 46A-6-101, et seq.

1242. West Virginia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the West Virginia Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

1243. Plaintiff and West Virginia Subclass members are "consumers," as defined by W. Va. Code § 46A-6-102(2).

1244. Marriott engaged in "consumer transactions," as defined by W. Va. Code § 46A-6-102(2).

1245. Marriott advertised, offered, or sold goods or services in West Virginia and engaged in trade or commerce directly or indirectly affecting the people of West Virginia, as

defined by W. Va. Code § 46A-6-102(6).

1246. Marriott engaged in unfair and deceptive business acts and practices in the conduct of trade or commerce, in violation of W. Va. Code § 46A-6-104, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and West Virginia Subclass members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and West Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and West Virginia Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and West Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and West Virginia Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and West Virginia Subclass members' Personal Information, including duties imposed by the FTC

Act, 15 U.S.C. § 45.

1247. 1358. Marriott's unfair and deceptive acts and practices also violated W. Va. Code § 46A-6-102(7), including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;
- b. Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised;
- d. Engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding;
- e. Using deception, fraud, false pretense, false promise or misrepresentation, or the concealment, suppression or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of goods or services, whether or not any person has in fact been misled, deceived or damaged thereby; and
- f. Advertising, displaying, publishing, distributing, or causing to be advertised, displayed, published, or distributed in any manner, statements and representations with regard to the sale of goods or the extension of consumer credit, which are false, misleading or deceptive or which omit to state material information which is necessary to make the statements therein not false, misleading or deceptive.

1248. Marriott's unfair and deceptive acts and practices were unreasonable when weighed against the need to develop or preserve business, and were injurious to the public interest, under W. Va. Code § 46A-6-101.

1249. Marriott's acts and practices were additionally "unfair" under W. Va. Code § 46A-6-104 because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to

consumers or to competition.

1250. The injury to consumers from Marriott's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and/or an unwarranted risk to the safety of their Personal Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1251. Consumers could not have reasonably avoided injury because Marriott's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Marriott created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1252. Marriott's inadequate data security had no countervailing benefit to consumers or to competition.

1253. Marriott's acts and practices were additionally "deceptive" under W. Va. Code § 46A-6-104 because Marriott made representations or omissions of material facts that misled or were likely to mislead reasonable consumers, including Plaintiff and West Virginia Subclass members.

1254. Marriott intended to mislead Plaintiff and West Virginia Subclass members and induce them to rely on its misrepresentations and omissions.

1255. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1256. Had Marriott disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the

law. Instead, Marriott held itself out as secure and was trusted with sensitive and valuable Personal Information regarding millions of consumers, including Plaintiff and the West Virginia Subclass.

1257. Marriott accepted the responsibility of being a “steward of data” while keeping the inadequate state of its security controls secret from the public.

1258. Plaintiff and the West Virginia Subclass members acted reasonably in relying on Marriott’s misrepresentations and omissions, the truth of which they could not have discovered.

1259. Marriott had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the Personal Information in its possession, and generally accepted professional standards. This duty arose because members of the public, including Plaintiff and the West Virginia Subclass, repose a trust and confidence in Marriott.

1260. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the West Virginia Subclass—and Marriott, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott.

1261. Marriott’s duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the West Virginia Subclass that contradicted these representations.

1262. Marriott’s omissions were legally presumed to be equivalent to active misrepresentations because Marriott intentionally prevented Plaintiff and West Virginia Subclass members from discovering the truth regarding Marriott’s inadequate data security.

1263. Marriott acted intentionally, knowingly, and maliciously to violate West Virginia’s

Consumer Credit and Protection Act, and recklessly disregarded Plaintiff and West Virginia Subclass members' rights. Marriott's unfair and deceptive acts and practices were likely to cause serious harm. Marriott's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1264. As a direct and proximate result of Marriott's unfair and deceptive acts or practices and Plaintiff and West Virginia Subclass members' purchase of goods or services, Plaintiff and West Virginia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1265. Marriott's violations present a continuing risk to Plaintiff and West Virginia Subclass members as well as to the general public.

1266. Plaintiff and West Virginia Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or \$200 per violation under W. Va. Code § 46A-6-106(a); restitution, injunctive and other equitable relief; punitive damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE WISCONSIN SUBCLASS

COUNT 78

NOTICE OF UNAUTHORIZED ACQUISITION OF PERSONAL INFORMATION,

Wis. Stat. §§ 134.98(2), et seq.

1267. Wisconsin Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wisconsin Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

1268. Marriott is a business that maintains or licenses Personal Information as defined by

Wis. Stat. § 134.98(2).

1269. Plaintiff's and Wisconsin Subclass members' PII includes Personal Information as covered under Wis. Stat. § 134.98(1)(b).

1270. Marriott is required to accurately notify Plaintiff and Wisconsin Subclass members if it knows that Personal Information in its possession has been acquired by a person whom it has not authorized to acquire the Personal Information within a reasonable time under Wis. Stat. §§ 134.98(2)-(3)(a).

1271. Because Marriott knew that Personal Information in its possession had been acquired by a person whom it has not authorized to acquire the Personal Information, Marriott had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wis. Stat. § 134.98(2).

1272. By failing to disclose the Marriott data breach in a timely and accurate manner, Marriott violated Wis. Stat. § 134.98(2).

1273. As a direct and proximate result of Marriott's violations of Wis. Stat. § 134.98(3)(a), Plaintiff and Wisconsin Subclass members suffered damages, as described above.

1274. Plaintiff and Wisconsin Subclass members seek relief under Wis. Stat. § 134.98, including actual damages and injunctive relief.

COUNT 79

WISCONSIN DECEPTIVE TRADE PRACTICES ACT,

Wis. Stat. § 100.18

1275. Wisconsin Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wisconsin Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

1276. Marriott is a "person, firm, corporation or association," as defined by Wis. Stat. § 100.18(1).

1277. Plaintiff and Wisconsin Subclass members are members of “the public,” as defined by Wis. Stat. § 100.18(1).

1278. With intent to sell, distribute, or increase consumption of merchandise, services, or anything else offered by Marriott to members of the public for sale, use, or distribution, Marriott made, published, circulated, placed before the public or caused (directly or indirectly) to be made, published, circulated, or placed before the public in Wisconsin advertisements, announcements, statements, and representations to the public which contained assertions, representations, or statements of fact which are untrue, deceptive, and/or misleading, in violation of Wis. Stat. § 100.18(1).

1279. Marriott also engaged in the above-described conduct as part of a plan or scheme, the purpose or effect of which was to sell, purchase, or use merchandise or services not as advertised, in violation of Wis. Stat. § 100.18(9).

1280. Marriott’s deceptive acts, practices, plans, and schemes include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Wisconsin Subclass members’ Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Wisconsin Subclass members’ Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Wisconsin Subclass members’ Personal Information, including by implementing and

maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Wisconsin Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Wisconsin Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Wisconsin Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1281. Marriott intended to mislead Plaintiff and Wisconsin Subclass members and induce them to rely on its misrepresentations and omissions.

1282. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

1283. Marriott had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the Personal Information in its possession, and generally accepted professional standards. This duty arose because members of the public, including Plaintiff and the Wisconsin Subclass, repose a trust and confidence in Marriott. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Wisconsin Subclass—and Marriott, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Marriott.

1284. Marriott's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its

systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Wisconsin Subclass that contradicted these representations.

1285. Marriott's failure to disclose the above-described facts is the same as actively representing that those facts do not exist.

1286. Marriott acted intentionally, knowingly, and maliciously to violate the Wisconsin Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Wisconsin Subclass members' rights. Past data breaches put Marriott on notice that its security and privacy protections were inadequate.

1287. As a direct and proximate result of Marriott's deceptive acts or practices, Plaintiff and Wisconsin Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1288. Marriott had an ongoing duty to all Marriott customers to refrain from deceptive acts, practices, plans, and schemes under Wis. Stat. § 100.18.

1289. Plaintiff and Wisconsin Subclass members seek all monetary and nonmonetary relief allowed by law, including damages, reasonable attorneys' fees, and costs under Wis. Stat. § 100.18(11)(b)(2), injunctive relief, and punitive damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, for themselves and Class Members, respectfully request that (i) this action be certified as a class action, (ii) Plaintiffs be designated the Class Representatives, and

(iii) Plaintiffs' counsel be appointed as Class Counsel. Plaintiffs, for themselves and Class Members, further request that upon final trial or hearing, judgment be awarded against Marriott, in Plaintiffs' favor for:

- A. compensatory and punitive damages in an amount to be determined by the trier of fact;
- B. declaratory and injunctive relief (as set forth above);
- C. attorneys' fees, litigation expenses and costs of suit incurred through the trial and any appeals of this case;
- D. pre- and post-judgment interest on any amounts awarded; and
- E. such other and further relief the Court deems just and proper.

JURY DEMAND

Plaintiffs, individually and on behalf of Class Members, respectfully demand a trial by jury on all of his claims and causes of action so triable.

Dated: December 19, 2018

Respectfully submitted,

/s/ Gary E. Mason

Gary E. Mason, Bar No. 15033

Whitfield Bryson & Mason LLP

5101 Wisconsin Avenue NW | Ste 305

Washington, DC 20016

Tel: 202-640-1168

Fax: 202-429-2294

gmason@wbmlp.com

Daniel S. Robinson (pro hac to be filed)

Wesley K. Polischuk (pro hac to be filed)

Michael W. Olson (pro hac to be filed)

Robinson Calcagnie, Inc.

19 Corporate Plaza Dr.

Newport Beach, CA 92660

Tel: 949-720-1288

Fax: 949-720-1292

drobinson@robinsonfirm.com

wpolischuk@robinsonfirm.com

moloson@robinsonfirm.com

Steven M. Pavsner, Esquire, Bar No. 01353
Veronica Byam Nannis, Bar No. 15679
Jay P. Holland, Bar No. 06015
Joseph, Greenwald & Laake, P.A.
6404 Ivy Lane, Suite 400
Greenbelt, Maryland 20770
Tel: 301-220-2200
Fax (301) 220-1214
spavsner@jgllaw.com
vnannis@jgllaw.com
jholland@jgllaw.com

Jeffrey S. Goldenberg (pro hac to be filed)
Goldenberg Schneider, LPA
One West Fourth Street, 18th Floor
Cincinnati, OH 45202
Tel: 513-345-8297
Fax: 513-345-8294
jgoldenberg@gs-legal.com

Charles E. Schaffer (pro hac to be filed)
Levin Sedran & Berman, LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Tel: 215-592-1500
Fax: 215-592-4663
cschaffer@lfsblaw.com

Greg Coleman (pro hac to be filed)
Greg Coleman Law PC
First Tennessee Plaza
Knoxville, TN 37929
Tel: 865-247-0080
Fax: 865-522-0049
greg@gregcolemanlaw.com

D. Greg Blankinship (pro hac to be filed)
Jeremiah Frei-Pearson (pro hac to be filed)
**Finkelstein, Blankinship,
Frei-Pearson & Garber, LLP**
445 Hamilton Avenue, Suite 605
White Plains, New York 10601
Tel: 914-298-3281
Fax: 914-824-1561
gblankinship@fbfglaw.com
jfrei-pearson@fbfglaw.com

Jay D. Miller, Bar No. 04653
Craig M. Silverman, Bar No. 16898
Law Offices of Peter G. Angelos, P.C.
One Charles Center
100 N. Charles Street, 20th Floor
Baltimore, MD 21201
Tel: (410) 649-2000
Fax: (410) 649-2101
jmiller@lawpga.com
csilverman@lawpga.com